IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPL. NO.:	09/978,224	
APPLICANT:	REUBEN BAHAR	Art Unit 2443
		Examiner: Asghar H. Bilgrami
FILED:	02/13/2003	Confirmation No. 4472
FOR:	"METHOD AND SYSTEM CONFIRMING PROPER RECEIPT OF E-MAIL TRANSMITTED VIA A COMMUNICATIONS NETWORK"	Attorney Docket No. 6589-A-7

FILED ON JULY 6, 2009 VIA EFS

BRIEF OF APPELLANT (SECOND APPEAL)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Brief of Appellant is in support of the Notice of Appeal filed in the Patent Office by the above-identified Applicant/Appellant (hereinafter, "Appellant") on May 4, 2009, appealing the final rejection of the Examiner dated February 3, 2009, finally rejecting claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348. Payment of the fee of $270.00 for filing the Appeal Brief, as set forth in § 41.20(b)(2) for a small entity, accompanies this filing. The Patent Office is hereby authorized to charge any additional fees required by this paper to Deposit Account No. 03-0088.

This Brief of Appellant sets forth the authorities and arguments on which Appellant relies to maintain this appeal. A Claims Appendix, setting forth the text of the claims involved in this appeal, is attached hereto. Also attached are appendices for evidence and related proceedings.

1. Real Party In Interest.

The real party in interest is the Appellant/inventor, namely, Reuben Bahar of West Hills, California. The claimed invention has not been assigned or licensed.

2. Related Appeals and Intereferences.

Appellant filed a Notice of Appeal in this application in August of 2007, along with a Brief of Appellant (Oct. 29, 2007) in support of such appeal, followed by a First Amended Brief of Appellant (Dec. 7, 2007). However, after Appellant filed his First Amended Appeal Brief, the Examiner re-opened prosecution of this application, and issued a further Office Action (Mar. 24, 2008), rather than filing an Examiner's Answer.

3. Status of Claims.

None of the pending claims are allowed or objected to. All of claims 1-348 are either: 1) rejected and being appealed; or 2) canceled, in accordance with the listing below:

Claims	Status
1-183	Canceled.
184-189	Rejected and being appealed.
190.	Canceled.
191-213	Rejected and being appealed.
214	Canceled.
215-229	Rejected and being appealed.
230	Canceled.

Claims	Status [continued from prior page]
231-234	Rejected and being appealed.
235	Canceled.
236-243	Rejected and being appealed.
244-247	Canceled.
248-255	Rejected and being appealed.
256-257	Canceled.
258-271	Rejected and being appealed.
272-278	Canceled.
279	Rejected and being appealed.
280-326	Canceled.
327-340	Rejected and being appealed.
341-345	Canceled.
346-348	Rejected and being appealed.

4. Status of Amendments.

After prosecution was re-opened in March of 2008, Appellant filed an Amendment (Sept. 29, 2008) in response to the non-final Office Action mailed March 24, 2008. Appellant's Amendment of Sept. 29, 2008 was entered by the Examiner.

After receiving the final Office Action mailed February 3, 2009, Appellant filed an Amendment After Final Rejection (May 4, 2009). The Amendment filed May 4, 2009 amended independent claims 236, 248 and 252 to cure formal defects raised by the Examiner in the final Office Action under 35 U.S.C. §101 (claims 248, 252), and under 35 U.S.C. §112, second paragraph (claim 236), and to place the present application in better form for appeal. The Examiner issued an Advisory Action Before the Filing of an Appeal Brief (May 14, 2009) indicating that Appellant's May 4, 2009 Amendment After Final Rejection had been entered.

5. **Summary of Claimed Subject Matter.**

Appellant has set forth below a concise explanation of the subject matter defined in each of the independent claims (236, 248, 252, 258, 260, 264, and 268) involved in the appeal, including references to the specification by page and line number, and to the drawings by reference characters, where appropriate.

Claim 236:

Claim 236 recites a method for verifying whether an e-mail message 12 was accessed by an intended recipient 20. In practicing such method, an e-mail message 12 is received at a recipient e-mail address. The recited method includes the step of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and prompts the accessing party 20 to input recipient data (see spec. p. 27, lines 6-23) before allowing access to such email message; the aforementioned recipient data includes identifying data related to the accessing party 20. The method of claim 236 also sends identifying data, for reference by sending party 10, to identify the party who accessed e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).

Claim 248:

Claim 248 recites a system for verifying whether an e-mail message 12 was accessed by an intended recipient. The system of claim 248 includes a recipient computer 14/21 connected to communications network 13 (see items 14 and 21 in Fig. 1, and see spec. p. 14, line 24 through p. 15, line 14, and p. 16, line 24 through p. 17, line 9); the recipient computer 14/21 is capable of receiving e-mail message 12 and includes data storage 17/24 for storing received e-mail message 12 (see items 17 and 24 in Fig. 1, and see spec. p. 17, lines 10-19).

The system of claim 248 also includes software (e.g., executable attachment file 12' in Fig. 1) that is capable of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2); upon detecting such access event, this software 12' prompts accessing party 20 to input recipient data before allowing access to e-mail message 12 (see spec. p. 27, lines 6-23). The recipient data inputed by accessing party 20 includes identifying data which identifies the accessing party 20 (e.g., see spec. p. 27, lines 13-17, and p. 29, lines 14-23) . The system of claim 248 also includes "means" (e.g., software) for sending identifying data to identify the party who accessed e-mail message 12 (see item 28 in Fig. 1; items 44 and 45 in Fig. 2, and see Figs. 3 and 4; also see, for example, spec. p. 19, lines 1-11).

Claim 252:

Claim 252 recites a system for verifying whether an e-mail message was accessed by an intended recipient. The system of claim 252 includes a recipient computer 14/21 connected to communications network 13 (see items 14 and 21 in Fig. 1, and see spec. p. 14, line 24 through p. 15, line 14, and p. 16, line 24 through p. 17, line 9); the recipient computer 14/21 is capable of receiving e-mail message 12 and includes data storage 17/24 for storing received e-mail message 12 (see items 17 and 24 in Fig. 1, and see spec. p. 17, lines 10-19).

The system of claim 252 further includes a "means" for recognizing biometric attributes of an individual (see spec. p. 29, line 14 through p. 30, line 23).

The system of claim 252 also includes software capable of detecting an access event (see spec. p. 17, line 20, through p. 18, line 2) and identifying an individual through utilization of inputted biometric attributes of said individual (see spec. p. 29, line 14 through p. 30, line 23).

Lastly, the system of claim 252 includes "means" (e.g., software) for sending data that identifies the party who accessed e-mail message 12 (see item 28 in Fig. 1; items 44 and 45 in Fig. 2, and see Figs. 3 and 4; also see, for example, spec. p. 19, lines 1-11).

Claim 258:

Claim 258 recites a method for verifying whether an e-mail message 12 was accessed by an intended recipient 20. In practicing such method, an e-mail message 12 is received at a recipient e-mail address. The recited method includes the step of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and prompts the accessing party 20 to input recipient data (see spec. p. 27, lines 6-23) before allowing the access to such email message by the accessing party 20; the aforementioned recipient data includes identifying data associated with the accessing party 20. The method of claim 258 also sends identifying data to identify the party who accessed the e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).

Claim 260:

Claim 260 recites a method for verifying whether an e-mail message 12 was accessed by an intended recipient 20. In practicing such method, an e-mail message 12 is received at a recipient e-mail address. The recited method includes the step of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 260 includes the further step of acquiring recipient data, wherein such recipient data is related to biometric identification of the accessing party 20 (see spec. p. 29, line 14 through p. 30, line 23). The method of claim 260 also permits email message 12 to be accessed after the recipient data is acquired.

The method of claim 260 also sends identifying data, related to biometric identification of the recipient, to identify the recipient of the e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).

Claim 264:

Claim 264 recites a method for verifying whether an e-mail message 12 was accessed by an intended recipient 20. In practicing such method, an e-mail message 12 is received at a recipient e-mail address. The method of claim 264 includes the step of utilizing biometric identification information to identify a recipient requesting access to the email message (see spec. p. 29, line 14 through p. 30, line 23).

The method of claim 264 further includes the step of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1), and permitting access to email message 12 after acquiring the biometric identification information. The method of claim 264 also sends recipient biometric identification information for confirming proper delivery of the e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).

Claim 268:

Claim 268 recites a method for verifying whether an e-mail message 12 was accessed by an intended recipient 20. In practicing such method, an e-mail message 12 is received at a recipient e-mail address. The method of claim 268 includes the further step of identifying a recipient requesting access to e-mail message 12 using biometric identification information associated with such recipient (see spec. p. 29, line 14 through p. 30, line 23).

The method of claim 268 further includes the step of detecting an access event (see spec. p. 17, line 20 through p. 18, line 2; and see items 18 and 25 in Fig. 1). The method of claim 268 also permits access to email message 12 after acquiring the biometric identification information. The method of claim 268 also sends recipient biometric identification information for confirming proper delivery of the e-mail message 12 (see spec. p. 23, lines 3-14, and p. 31, lines 11-15).

6. Grounds of Rejection to be Reviewed on Appeal:

a. Did the Patent Examiner error in rejecting claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348, as describing subject matter that would have been obvious to those skilled in the art under 35 U.S.C. Section 103(a) based upon Choi (U.S. Pat. No. 6,629,131), Flynn (U.S. Pat. No. 6,618,747), and Kanevsky (U.S. Pat. No. 6,836,846)?

7. Argument.

A. The Cited Prior Art.

Choi (U.S. Patent No. 6,629,131):

The cited '131 patent to Choi describes a method for confirming receipt of an email message. Choi's method assigns a unique code to an e-mail message sent by a sender, and records the unique code in a database. This unique code is generated at the sender's end of the transmission and is attached to the e-mail message as a "CGI executive program". Upon access of the email message by the recipient, Choi's method sends the unique code that was attached to the message back to the web server of the sender; this step is performed by the automatic execution of the attached "CGI executive program" executed at the receiver's end when the e-mail message is

received by the receiver. A comparison is made of the unique code received from the CGI executive program and the unique code previously recorded when the sender first sent the email message. If the two codes are identical, then confirmation information is sent to the sender indicating that the email message has been accessed.

Flynn (U.S. Patent No. 6,618,747):

The cited '747 patent to Flynn discloses a system wherein an intended recipient is notified that an email message has been posted at a third party web host for such recipient. Notification of the existence of the posted e-mail is communicated by the third party web host which sends an e-mail message informing the recipient that an e-mail message is waiting for the recipient at a specified third party web host URL. Included in this e-mail message is the third party URL address where the posted message is located. If the intended recipient accesses the message, a confirmation notice is sent to the sender to confirm that the message was downloaded. Flynn describes the URL address at which the posted e-mail message is posted on the third party web host as a "unique call address" (assigned by Flynn's Web Server 24) that provides access to an e-mail message stored at such unique call address on the third party Web server. When the email message is downloaded by the requesting party, Flynn's system sends a confirmation of receipt notice that includes the address to which the email was downloaded, the time it was downloaded, and optionally, a compressed copy of the original message.

Kanevsky (U.S. Pat. No. 6,836,846):

Kanevsky describes a "system and methodology for controlling access to e-mail data content present in e-mail messages; see Kanevsky, col. 1, lines 7-10. Kanevsky states that "[s]enders of E-mail messages often want the message to be retrieved and accessed by the intended recipient ***and not made available to anybody else to access***." (emphasis added); see Kanevsky, col. 1, lines 13-15. Indeed, Kanevsky states that it would be "... be highly desirable to provide a system and method that enables a sender to control access to e-mail data after sending the e-mail message to the intended recipient", and further states that it is the primary objective of the invention "... to provide a system and method for enabling a sender to control access to e-mail and electronic information content after sending the e-mail message to an intended recipient"; see Kanevsky, col. 1, lines 24-26 and 29-32.

To accomplish Kanevsky's stated objective, Kanevsky discloses two methods of ensuring that the person requesting access to the e-mail message is the intended recipient. First, a remote authentication process is disclosed wherein the sender of an e-mail assigns an identity verification requirement (e.g. biometric identification) to such e-mail. Upon receipt of such e-mail, the receiving party must identify himself/herself via a biometric attribute such as a fingerprint scan. That biometric data is then communicated back to the sender of the e-mail. The returned biometric data is processed by doing a query in the sender's database. If the returned biometric data is verified against the sender's database, then the sender can grant to such recipient access to the original message by sending a further message granting such access (see Kanevsky, at col. 6, lines 1-26).

Kanevsky also describes a local authentication process wherein the sender of an e-mail assigns an identity verification requirement (e.g. biometric identification) to such e-mail, along with expected authentication data. Upon receipt of such e-mail, the receiving party must identify himself/herself via a biometric attribute such as a fingerprint scan. That biometric data is then compared locally on the recipient's computer with the expected authentication data packaged with such e-mail message by the sender. The biometric data input by the person requesting access is compared to the expected biometric data packaged with the message by the sender. Only if they match is the person requesting access permitted to access such e-mail message (see Kanevsky, col. 6, lines 27-47).

In summary, Kanevsky teaches a method for authenticating the identity of the party requesting access of an e-mail by verifying their identity before allowing access to the e-mail. If the recipient's identity is not that of the intended recipient, then access to the e-mail is altogether denied by Kanevsky's system. In other words, Kavensky ensures that the recipient intended by the sender is the only party that can access the e-mail. On the other hand, the Kanevsky system cannot identify persons requesting access who are not the recipient intended by the sender, nor will it allow them access to such e-mail.

B. The Examiner's Rejections:

Within the final Office Action mailed February 3, 2009, the Patent Examiner finally rejected claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348 under Section 103(a). The Examiner rejected such claims as describing subject matter considered to be unpatentable over Choi (U.S. Pat. No. 6,629,131), Flynn (U.S. Pat. No.

6,618,747), and Kanevsky (U.S. Pat. No. 6,836,846). With respect to independent claims 236, 248, 252, 258, 260, 264, and 268, the Examiner argued that it would have been obvious to one skilled in the art, at the time the invention was made, to modify Choi to: (1) detect an access event; (2) prompt the requesting party to input identifying data; and (3) to permit the requested access after acquiring such identifying data; all as purportedly disclosed by Kanevsky. In addition, the Examiner contends that it would have been obvious from Flynn to send identifying data (relating to the party associated with the access request) for reference by a sending party to identify the party who accessed the email.[1]

C. The Cited Patents Do Not Render Obvious the Appealed Claims:

Claim 236:

Claim 236 sets forth a method for verifying whether an e-mail was accessed by an intended recipient. The recited method includes the step of "detecting an access event, and prompting the party associated with said access event to input recipient data prior to allowing the requested access". Claim 236 states that the "recipient data" (which the recipient must input before being allowed to access the e-mail message) includes "identifying data related to the party associated with said requested access". Further, claim 236 recites the step of "permitting said e-mail to be accessed after the party associated with said access event inputs said recipient data".

---

[1] While the Examiner states, in the final Office Action (see page 5) that Kanevsky did not explicitly disclose sending identifying data related to the party requesting access for reference by the sender, Appellant has pointed out above that Kanevsky's remote authorization method does just that.

The Patent Examiner rejected claim 236 within paragraph 10 of the final Office Action mailed February 3. 2009, which starts on page 3 thereof. Within such paragraph 10, the Patent Examiner stated the following:

> "10. As per claims .... 236, ... Choi disclosed a method for verifying whether an e-mail received by a recipient was accessed by an intended recipient ... However, Choi did not explicitly disclose b) detecting an access event, and prompting the party associated with said event to input recipient data prior to allowing the requested access... ".

Thus, the Examiner concedes that Choi does not disclose or suggest the step of detecting an access event, nor the step of prompting the party associated with the access event to input recipient data prior to allowing the requested access.

At page 4 of the final Office Action, the Examiner argues that Kanevsky discloses detection of an access event, and conditioning access upon input of recipient data. More specifically, the Examiner states:

> "In the same field of endeavor Kanevsky et al disclosed b) detecting an access event, and prompting the party associated with said event to input recipient data prior to allowing the requested access (col. 6, lines 1-26) ... e) permitting said e-mail to be accessed after the party associated with the said access event inputs said recipient data (col. 7, lines 7-10)."

Still at page 4 of the final Office Action, the Examiner argued that it would have been obvious to one skilled in the art to modify Choi to detect an access event, in accordance with Kanevksy, in order to verify whether the email message was delivered to the intended recipient.

The problem with the Examiner's argument is that Kanevsky does <u>not</u> permit the e-mail message to be accessed <u>unless</u> either: 1) the sender grants to the recipient the right to access the

first email message after reviewing the credentials returned by the recipient and thereafter sending a second message granting such access (see Kanevsky specification at col. 6, lines 1-26); or 2) the sender attaches expected authentication data to the email message, and the identification information entered by the recipient matches the expected authentication data forwarded by the sender (see Kanevsky specification at col. 6, lines 27-47).

In contrast, claim 236 recites the step of "permitting said e-mail to be accessed after the party associated with said access event inputs said recipient data", irrespective of whether such party is the intended recipient or not, without the need for the sender to authenticate the recipient's identification, and without the need for a comparison between expected authentication data and identification information entered by the recipient. In other words, in the invention of claim 236, permission to access the email message is unconditional, assuming that the party requesting access has input recipient data.

As noted above, Kanevsky's method requires verification that the identity of the party requesting access to the email matches the identity of the intended recipient before allowing access to the e-mail. If the identity of the requesting party does not match the sender's intended recipient, then access to the e-mail is altogether denied by Kanevsky; only if the party seeking access submits identification specified by the sender will Kanevsky permit access to the e-mail. On the other hand, Kanevsky cannot identify persons requesting access who are not the recipient intended by the sender, nor will Kanevsky permit access to such e-mail in such instances.

Thus, even if it were "obvious" to modify Choi, as the Examiner contends, to incorporate the teachings of Kanevsky, which Applicant does not concede, such a combination would nonetheless fail to achieve the method recited in claim 236, which permits any and all parties to

access an e-mail (both intended and unintended), provided that such party first inputs identifying recipient data. The method of claim 236 does not condition access upon the identity of the party requesting access, but simply discovers the identity of the person requesting access before the requesting party gains such access. The method of claim 236 is much less complicated, and more practical, than the system taught by Kanevsky.

The difference between the method of claim 236 and the Kanevsky disclosure might best be illustrated with the aid of an example. Suppose that a sender of an e-mail message is attempting to send a message wherein the intended recipient is generally the "accounting" department of a company. In this case, it is likely that several employees working in the "accounting" department would be authorized to access e-mail messages sent to the general "accounting" mailbox of the company. All that would be important to the sender is to confirm that someone working at the firm's "accounting" department accessed the e-mail message, along with an identification of that person. Using the system of claim 236, anyone in the accounting department of the company could open the e-mail, and as a result, a confirmation receipt (including the identity of such person) can be generated. In contrast, using Kanevsky's method, only a designated recipient would be able to access the e-mail; other un-designated individuals, who would otherwise be able to handle the incoming e-mail, would not be able to access the incoming e-mail message.

Thus, the method recited by claim 236 would not be obvious even if one were to modify the Choi's disclosure in accordance with the teachings of Kanevksy as proposed by the Examiner. The Examiner's rejection of claim 236 is not supported by the cited references and should be reversed.

Claims 248, 252, 258, 260, 264, 268:

Appellant's remarks, set forth above and directed to rejected claim 236, apply with equal force relative to the rejection of claims 248, 252, 258, 260, 264 and 268. In each instance, as will be demonstrated below, these independent claims permit access to a received e-mail message so long as the party requesting access has identified himself or herself:

- claim 248 recites that "... said software further permits said e-mail to be accessed after the party associated with said access event inputs said recipient data ...";

- claim 252 recites that "... said software permitting said e-mail to be accessed after input of said biometric attributes of the individual associated with said access event ...";

- claim 258 recites the step of "... permitting said e-mail to be accessed after the party that requested said access inputs said recipient data ...";

- claim 260 recites the step of "... permitting said e-mail to be accessed after acquiring said recipient data ...";

- claim 264 recites the step of "... permitting said e-mail to be accessed after acquiring said biometric identification ..."; and

- claim 268 recites the step of "... permitting said e-mail to be accessed after acquiring said biometric identification ...".

In each case, the claim requires an element or step wherein access to the e-mail message is permitted to the party requesting access once such party has been identified. While the Examiner relies upon Kanevsky to teach the concept of detecting an access event, Kanevsky also teaches the denial of access to the e-mail message unless the identity of the requesting party matches unique authentication data provided by the sender.

Non-Obviousness

It is not appropriate to pick and choose only so much of the Kanevsky disclosure as would arguably support the Examiner's rejection, while ignoring the remainder of Kanevsky's disclosure. See *In re Wesslau*, 353 F.2d 238, 241, 147 USPQ 391, 393 (CCPA 1965) ["It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art ..."]; *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ2d 1780, 1783 (Fed. Cir. 1988) [impermissible to "use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention."].

Kanevksy actually teaches away from the claimed invention because it would lead one skilled in the art away from the path chosen, and claimed, by Appellant. Claims 236, 248, 252, 258, 260, 264 and 268 all recite that access to the e-mail message is permitted once the party requesting access party inputs recipient data (see claims 236, 248, 258, 260), biometric attributes of said individual (see claim 252), or biometric identification (see claims 264 and 268). In contrast, Kanevsky teaches that access is permitted only when the party requesting access matches the intended recipient. A cited reference "teaches away" from the claimed invention when a person of ordinary skill, upon reading the reference, would be ... led in a direction divergent from the path that was taken by the applicant. *In re Kubin*, 561 F3d 1351, 90 USPQ2d 1417, 1421 (Fed. Cir. 2009), citing *In re Gurley*, 27 F.3d 551, 553 [31 USPQ2d 1130] (Fed. Cir. 1994). Where the prior art teaches away from the claimed invention, the claimed invention is more likely to be non-

obvious. *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1739–40, 82 USPQ2d 1385 (U.S. 2007).

8. Conclusion:

Accordingly, Appellant submits that the appealed independent claims 236, 248, 252, 258, 260, 264, and 268, and those appealed claims dependent therefrom, define subject matter that is patentably distinguishable over the applied prior art, and requests the Board to reverse the rejection of appealed claims 184-189, 191-213, 215-229, 231-234, 236-243, 248-255, 258-271, 279, 327-340, and 346-348.

Respectfully submitted,

CAHILL & GLAZER P.L.C.

Marvin A. Glazer
Registration No. 28,801

2141 East Highland Ave., Suite 155
Phoenix, Arizona 85016
Ph. (602) 956-7000
Fax (602) 495-9475
Docket No. 6589-A-7

CLAIMS APPENDIX (Claims Involved In The Appeal)

1. - 183. Canceled.

184. The method as recited in claim 258 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

185. The method as in claim 236, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

186. The method as in claim 236, wherein said access event comprises access of an e-mail account associated with said recipient e-mail address.

187. The method as in claim 236, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

188. The method as in claim 236, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail, the executable attachment file having a first module for prompting the party who requested said access event to enter recipient data; and

and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file.

189. The method as in claim 188, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and further comprising the step of automatically executing the second module upon delivery of the attachment file to the recipient e-mail address.

190. Canceled.

191. The method as in claim 236, wherein said recipient e-mail address is associated with a recipient computer.

192. The method as in claim 191, wherein said recipient computer is a server of a service provider.

193. The method as in claim 191, wherein said recipient computer is a user system that is directly accessible by a recipient, said user system including electronic mail processing software.

194. The method as in claim 236, wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

195. The method as in claim 236, wherein said inputted recipient data comprises identity information that identifies an individual.

196. The method as in claim 195, wherein said identity information pertains to biometric identification.

197. The method as in claim 196 further comprising the step of recognizing biometric attributes of an individual.

198. The method as in claim 195, wherein said identity information includes alphanumeric text identification information.

199. The method as in claim 236, wherein said inputted recipient data comprises information that identifies a business.

200. The method as in claim 236, wherein said inputted recipient data comprises information that identifies an organization.

201. The method as in claim 236, wherein said inputted recipient data comprises a computer generated user code.

202. The method as in claim 236 further including the step of sending access event data of attendant conditions of said access event.

203. The method as in claim 236, wherein said recipient is an individual.

204. The method as in claim 236, wherein said recipient is a business.

205. The method as in claim 236, wherein said recipient is an organization.

206. The method as in claim 236, wherein said inputted recipient data is used to verify proper delivery of legal documents.

207. The method as in claim 236, wherein said inputted recipient data is used to verify proper delivery of confidential documents.

208. The method recited by claim 260 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the acquired recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the acquired recipient data contained with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

209. The method as in claim 260, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

210. The method as in claim 260, wherein said access event comprises access of an e-mail account associated with said recipient e-mail address.

211. The method as in claim 260, wherein said access event comprises activation of e-mail processing software associated with said recipient e-mail address.

212. The method as in claim 260, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail, the

executable attachment file having a first module for acquiring recipient data that is related to biometric identification of the recipient, and

wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file.

213. The method as in claim 212, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and further comprising the step of:

automatically executing the second module upon delivery of the attachment file to the recipient e-mail address.

214. Canceled.

215. The method as in claim 260, wherein said recipient e-mail address is associated with a recipient computer.

216. The method as in claim 215, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

217. The method as in claim 215, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

218. The method as in claim 260, wherein said acquired recipient data is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code,

or a combination thereof.

219. The method as in claim 260, wherein said acquired recipient data comprises identity information that identifies an individual.

220. The method as in claim 260 further comprising means for recognizing biometric attributes of an individual.

221. The method as in claim 260, wherein said acquired recipient data comprises information that identifies a business.

222. The method as in claim 260, wherein said acquired recipient data comprises information that identifies an organization.

223. The method as in claim 260, wherein said acquired recipient data comprises a computer generated user code.

224. The method as in claim 260 further including the step of sending access event data of conditions attendant said access event.

225. The method as in claim 260, wherein said recipient is an individual.

226. The method as in claim 260, wherein said recipient is a business.

227. The method as in claim 260, wherein said recipient is an organization.

228. The method as in claim 260, wherein said sent recipient data is used to verify proper delivery of legal documents.

229. The method as in claim 260, wherein said sent recipient data is used to verify proper delivery of confidential documents.

230. Canceled.

231. The method as in claim 260, wherein said recipient data is acquired as a requisite condition for permitting access to said delivered e-mail.

232. The method as in claim 260, wherein said recipient data is acquired as a requisite condition for permitting access to said recipient e-mail address.

233. The method as in claim 260, wherein said recipient data is acquired as a requisite condition for operating a remote user computer, said remote user computer being operable to gain access to said recipient e-mail address.

234. The method as in claim 260, wherein said recipient data is comprised of alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute of said recipient.

235. Canceled.

236. A method for verifying whether an e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail at a recipient e-mail address;

b) detecting an access event, and prompting the party associated with said access event to input recipient data prior to allowing the requested access, said recipient data including identifying data related to the party associated with said requested access;

c) permitting said e-mail to be accessed after the party associated with said access event inputs said recipient data; and

d) sending identifying data relating to the party associated with said access event for reference by a sending party to identify the party who accessed said e-mail.

237. The method recited by claim 264 wherein the step of sending data that identifies said recipient for confirming proper delivery of said e-mail includes the steps of :

a) generating a confirmation of receipt notice wherein the data that identifies the recipient is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the data that identifies the recipient that is included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

238. The method as in claim 264, wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

239. The method as in claim 264, wherein the data that identifies said recipient is comprised of alphanumeric text, said alphanumeric text being associated with ~~the~~ at least one biometric attribute of said recipient.

240. The method as in claim 264 further including the step of recognizing biometric attributes of an individual.

241. The method as in claim 264, wherein said data that identifies said recipient comprises identity information that identifies an individual.

242. The method as in claim 264, wherein said data that identifies said recipient comprises information that identifies a business.

243. The method as in claim 264, wherein said data that identifies said recipient comprises information that identifies an organization.

244. - 247. Canceled.

248. A system for verifying whether e-mail received by a recipient was accessed by an intended recipient, said system comprising:

a) a recipient computer connected to a communications network, said recipient computer capable of receiving an e-mail and further having data storage for storing said received e-mail;

b) software on a computer storage medium capable of detecting an access event, wherein, upon detecting said access event, said software prompts the party associated with said access event to input recipient data prior to allowing the requested access and wherein said software further permits said e-mail to be accessed after the party associated with said access event inputs said recipient data, said recipient data comprising identifying data related to the party associated with said requested access; and

c) means for sending identifying data relating to the party associated with said access event to identify the party who accessed said e-mail.

249. The system as in claim 248, wherein said access event comprises access of a delivered e-mail.

250. The system as in claim 248, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

251. The system as in claim 248, wherein said access event comprises activation of ~~the~~ e-mail processing software associated with the e-mail address to which said e-mail was delivered.

252. A system for verifying whether e-mail received by a recipient was accessed by an intended recipient, said system comprising:

a) a recipient computer connected to a communications network, said recipient computer being capable of receiving an e-mail and further having data storage for storing said received e-mail;

b) biometric identification means for recognizing biometric attributes of an individual;

c) software on a computer storage medium capable of detecting an access event and identifying an individual associated with said access event through utilization of inputted biometric attributes of said individual, said software permitting said e-mail to be accessed after input of said biometric attributes of the individual associated with said access event; and

d) means for sending data that identifies said individual for identifying the party who accessed said e-mail.

253. The system as in claim 252, wherein said access event comprises access of a delivered e-mail.

254. The system as in claim 252, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

255. The system as in claim 252, wherein said access event comprises activation of ~~the~~ e-mail processing software associated with the e-mail address to which said e-mail was delivered.

256. - 257. Canceled.

258. A method for verifying whether an e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) detecting an access event, and prompting the party that requested said access to input recipient data prior to allowing the requested access, said recipient data including identifying data that is associated with the party that requested said access;

c) permitting said e-mail to be accessed after the party that requested said access inputs said recipient data; and

d) sending identifying data relating to the party that requested said access event to identify the party who accessed said e-mail.

259. The method recited by claim 236 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

260. A method for verifying whether e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) detecting an access event;

c) acquiring recipient data that is related to biometric identification of the recipient;

d) permitting said e-mail to be accessed after acquiring said recipient data; and

e) sending identifying data related to biometric identification of said recipient for identifying the recipient of said e-mail.

261. The method as recited in claim 260 wherein said recipient data is acquired prior to said access event.

262. The method as recited in claim 260 wherein said recipient data is acquired after said access event.

263. The method as recited in claim 260 wherein said recipient data is sent to an e-mail address.

264. A method for verifying whether e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) identifying a recipient utilizing biometric identification;

c) detecting an access event;

d) permitting said e-mail to be accessed after acquiring said biometric identification; and

e) sending data related to said biometric identification of said recipient for confirming proper delivery of said e-mail.

265. The method as recited in claim 264 wherein said recipient is identified prior to said access event.

266. The method as recited in claim 264 wherein said recipient is identified after said access event.

267. The method as recited in claim 264 wherein said data that identifies said recipient is sent to an e-mail address.

268. A method for verifying whether e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) identifying a recipient in association with biometric identification;

c) detecting an access event;

d) permitting said e-mail to be accessed after acquiring said biometric identification; and

e) sending data related to said biometric identification of said recipient for confirming proper delivery of said e-mail.

269. The method as in claim 268 wherein said recipient is identified prior to said access event.

270. The method as in claim 268 wherein said recipient is identified after said access event.

271. The method as in claim 268 wherein said data that identifies said recipient is sent to an e-mail address.

272. - 278. Canceled.

279. The system as in claim 252, wherein said data that identifies said individual for confirming proper delivery of said e-mail is sent to an e-mail address.

280. - 326. Canceled.

327. The method as in claim 236, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

328. The method as in claim 236, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

329. The method as in claim 236 wherein the party that is associated with said access event is an individual.

330. The method as in claim 236 wherein the party that is associated with said access event is a business.

331. The method as in claim 236 wherein the party that is associated with said access event is an organization.

332. The method as in claim 258 wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

333. The method as in claim 184, wherein said confirmation of receipt notice is sent to an e-mail address.

334. The method as in claim 258, wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

335. The method as in claim 208, wherein said confirmation of receipt notice is sent to an e-mail address.

336. The method as in claim 260, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

337. The method as in claim 219, wherein said identity information includes alphanumeric text identification.

338. The method as in claim 237, wherein said confirmation of receipt notice is sent to an e-mail address.

339. The method as in claim 268 , wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

340. The method as in claim 268 further comprising the step of recognizing biometric attributes of an individual.

341. - 345. Canceled.

346. The system as in claim 248, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

347. The system as in claim 252, wherein said individual is identified prior to said access event.

348. The system as in claim 252, wherein said individual is identified after said access event.

EVIDENCE APPENDIX

In regard to this Appeal, Appellant does not rely upon any evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131 or 1.132.

The Patent Examiner has relied upon U.S. Pat. No. 6,629,131 (Choi); U.S. Pat. No. 6,618,747 (Flynn), and U.S. Pat. No. 6,836,846 (Kanevsky), and Appellant has included remarks in the foregoing Brief of Appellant directed to such patent references. Accordingly, copies of the Choi, Flynn, and Kanevsky patents are attached hereto for the convenience of the Board.

US006629131B1

(12) **United States Patent**
Choi

(10) **Patent No.: US 6,629,131 B1**
(45) **Date of Patent: Sep. 30, 2003**

(54) **REGISTRATION MAIL SYSTEM WITH A SENT E-MAIL CHECK FUNCTION ON INTERNET AND METHOD FOR THE SAME**

(75) Inventor: **Woo Jin Choi**, Seoul (KR)

(73) Assignee: **Nexen Co., Ltd.**, Seoul (KR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/390,666**

(22) Filed: **Sep. 7, 1999**

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/206**; 709/207; 709/311; 707/104.1; 379/93.01; 379/93.24

(58) **Field of Search** 709/206, 207, 709/311; 379/93.01, 93.24; 707/104.1

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,781,901	A *	7/1998	Kuzma	358/402
6,108,688	A *	8/2000	Nielsen	709/206
6,175,859	B1 *	1/2001	Mohler	709/206
6,185,551	B1 *	2/2001	Birrell et al.	707/102
6,202,086	B1 *	3/2001	Maruyama et al.	358/434
6,226,670	B1 *	5/2001	Ueno et al.	340/10.1
6,289,212	B1 *	9/2001	Stein et al.	455/412
6,308,206	B1 *	10/2001	Singh	709/223
6,314,454	B1 *	11/2001	Wang et al.	358/402
6,332,164	B1 *	12/2001	Jain	709/203
6,393,456	B1 *	5/2002	Ambler et al.	709/200

* cited by examiner

Primary Examiner—Zarni Maung
Assistant Examiner—Jinsong Hu
(74) *Attorney, Agent, or Firm*—Schweitzer Cornman Gross & Bondell LLP

(57) **ABSTRACT**

An electronic mailing method on the Internet with a function of reception confirmation is described. The method is comprising the steps of (a) assigning a unique code to the e-mail of a sender and recording the unique code in a database; (b) attaching to the e-mail a CGI executive program that automatically sends the unique code to the web server of the sender when the receiver receives the e-mail; (c) sending the unique code to the web server of the sender by the automatic execution of the CGI executive program when the e-mail is received by the receiver; and (d) comparing the unique code sent in the step (c) and the unique code recorded in the step (a) and, if they are identical, sending reception confirmation information to the sender.

3 Claims, 5 Drawing Sheets

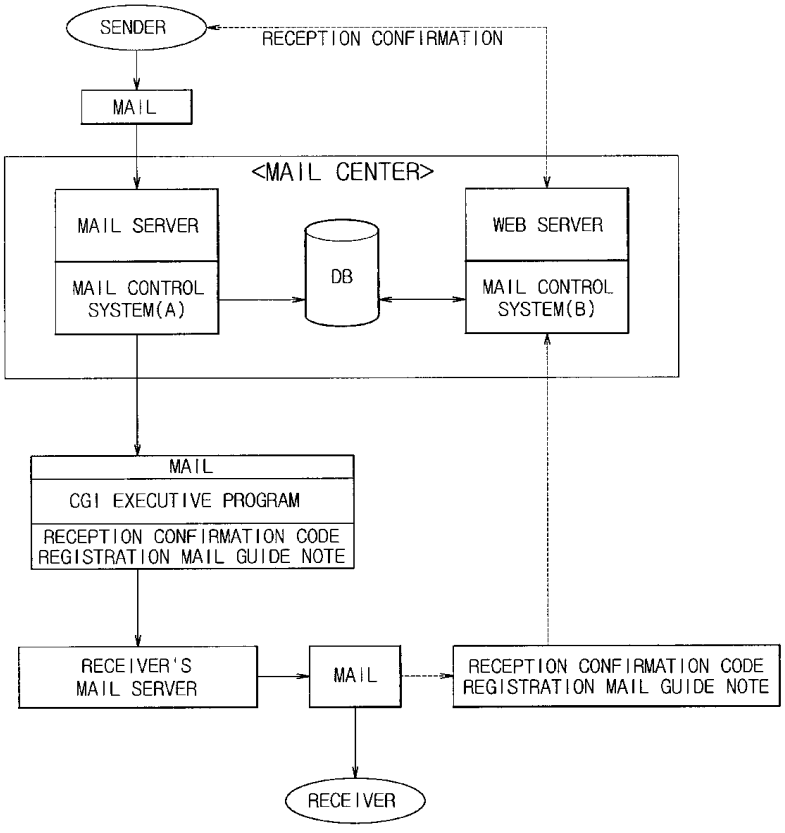


Fig.1

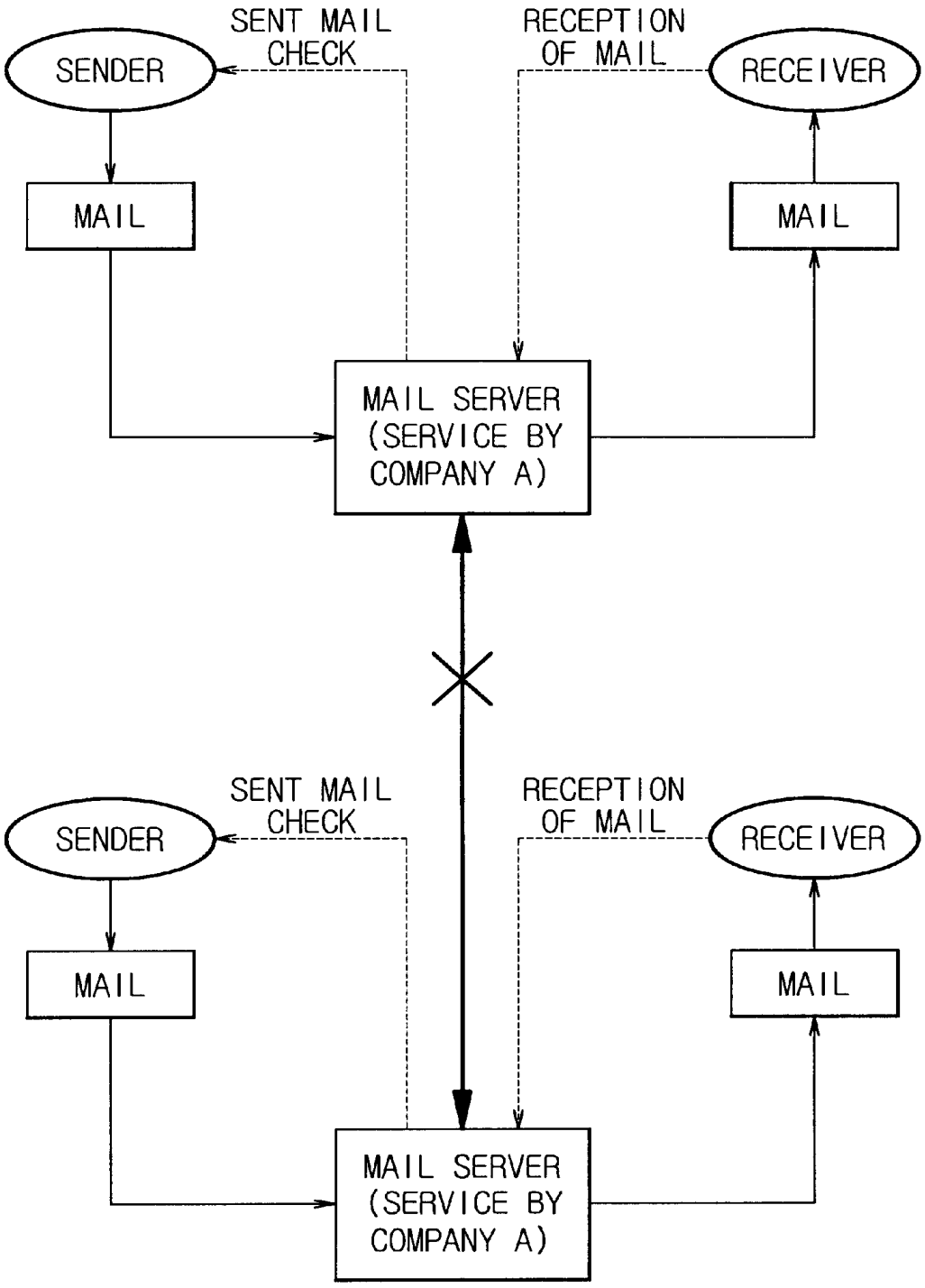

SENT MAIL CHECK
RECEPTION OF MAIL
SENDER
RECEIVER
MAIL
MAIL
MAIL SERVER (SERVICE BY COMPANY A)
SENT MAIL CHECK
RECEPTION OF MAIL
SENDER
RECEIVER
MAIL
MAIL
MAIL SERVER (SERVICE BY COMPANY A)

Fig.2

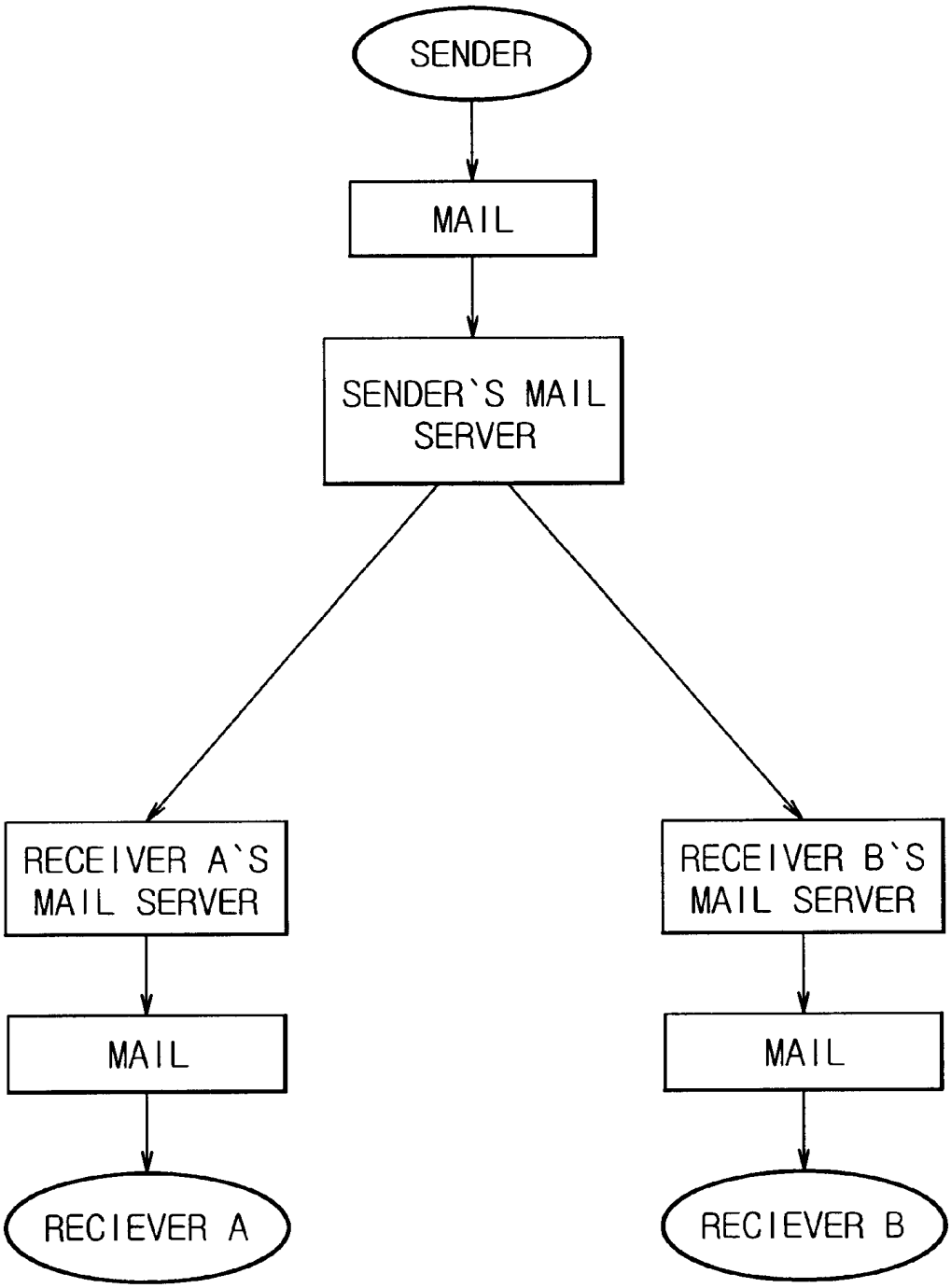

SENDER
MAIL
SENDER`S MAIL SERVER
RECEIVER A`S MAIL SERVER
RECEIVER B`S MAIL SERVER
MAIL
MAIL
RECIEVER A
RECIEVER B

Fig.3

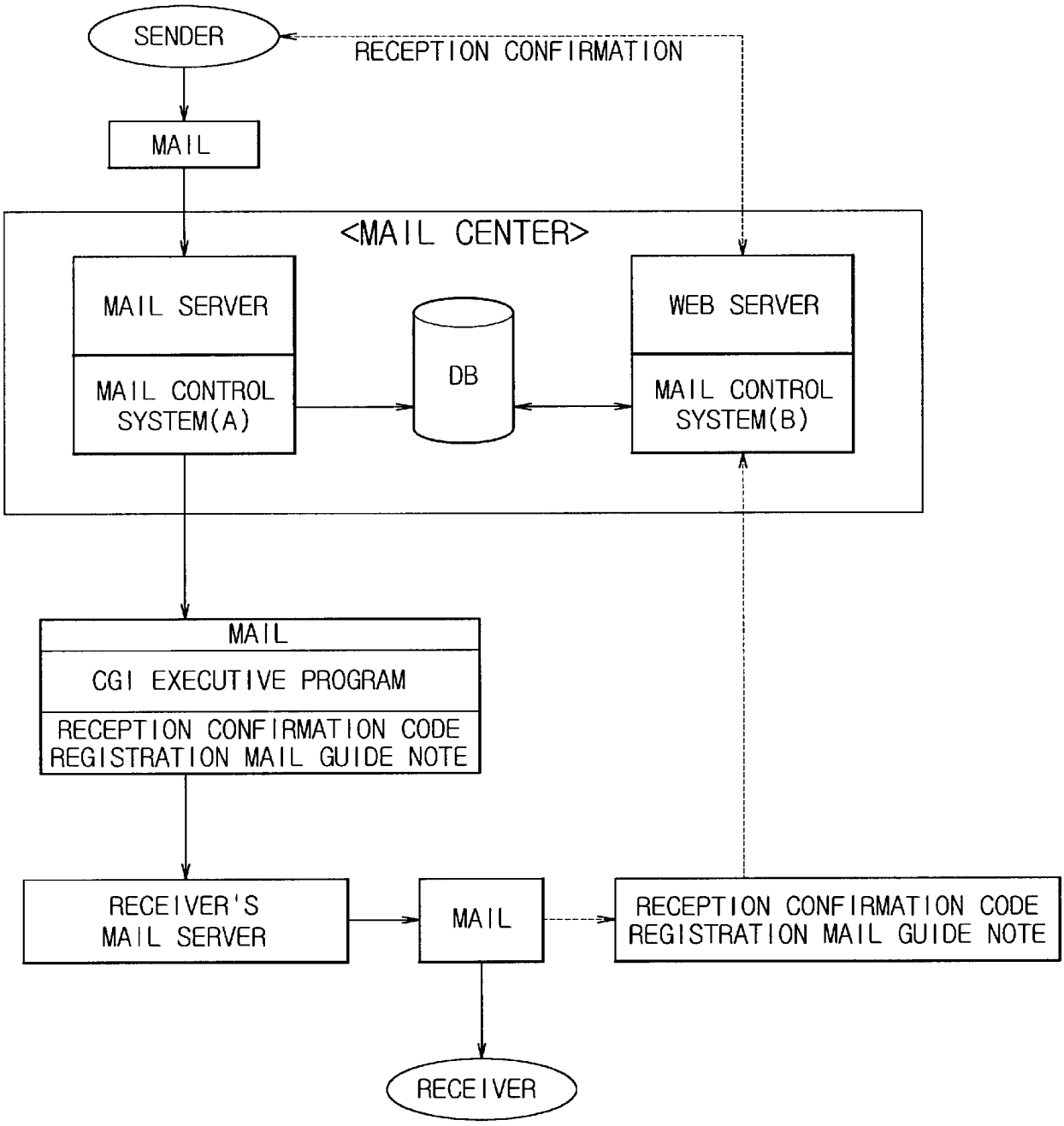

SENDER
RECEPTION CONFIRMATION
MAIL
<MAIL CENTER>
MAIL SERVER
MAIL CONTROL SYSTEM(A)
DB
WEB SERVER
MAIL CONTROL SYSTEM(B)
MAIL
CGI EXECUTIVE PROGRAM
RECEPTION CONFIRMATION CODE REGISTRATION MAIL GUIDE NOTE
RECEIVER'S MAIL SERVER
MAIL
RECEPTION CONFIRMATION CODE REGISTRATION MAIL GUIDE NOTE
RECEIVER

Fig.4

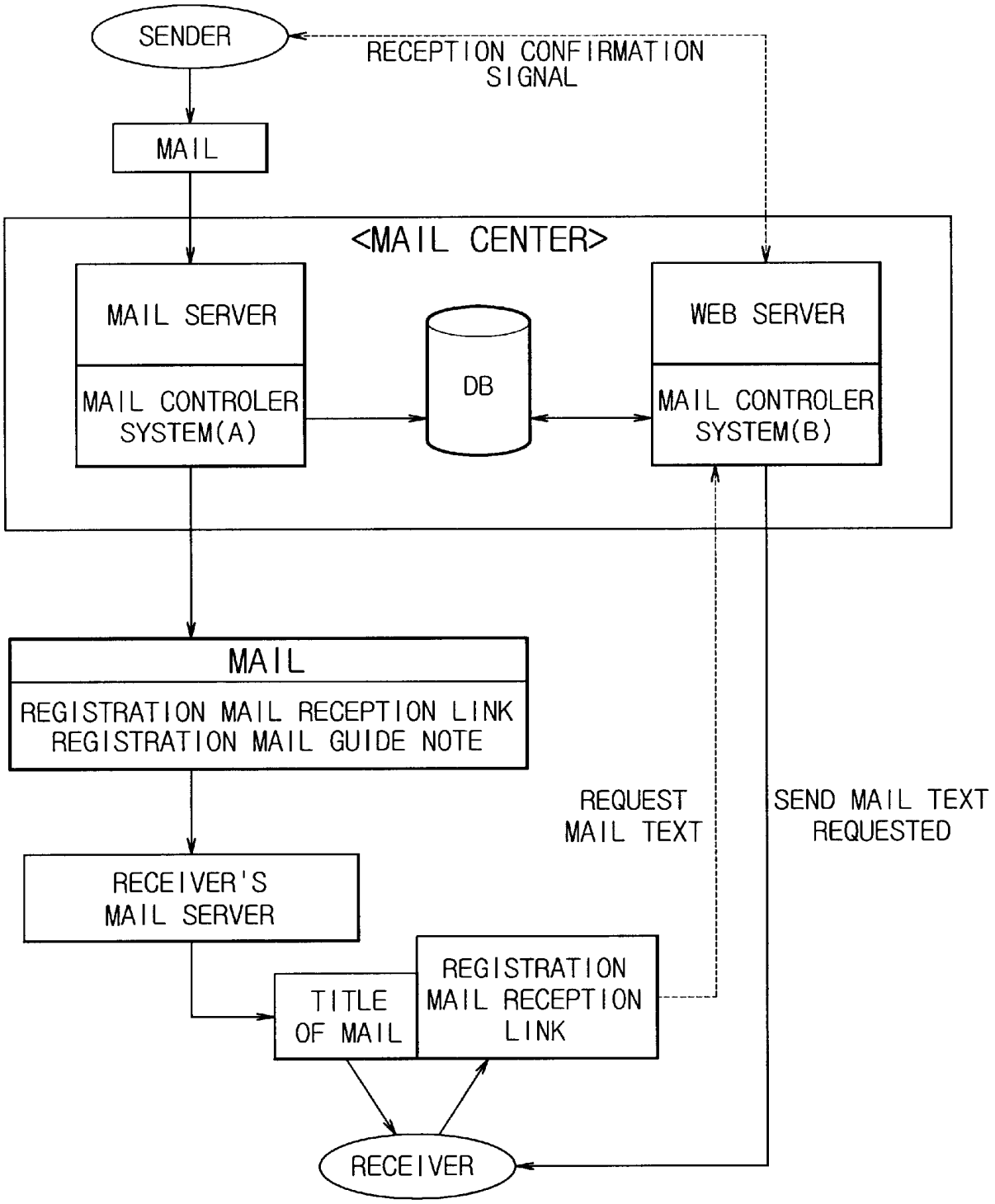
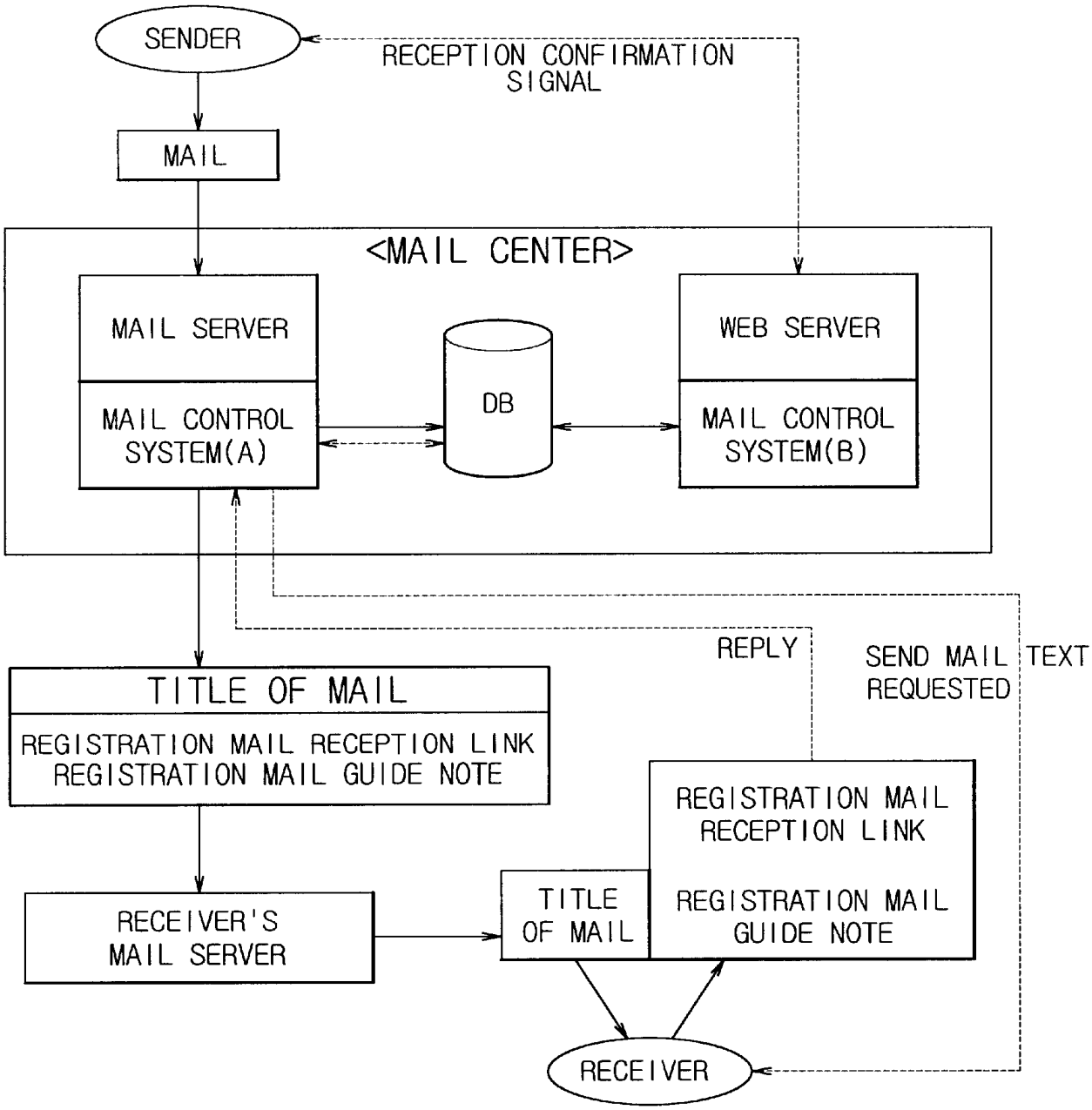

SENDER
RECEPTION CONFIRMATION SIGNAL
MAIL
<MAIL CENTER>
MAIL SERVER
MAIL CONTROLER SYSTEM(A)
DB
WEB SERVER
MAIL CONTROLER SYSTEM(B)
MAIL
REGISTRATION MAIL RECEPTION LINK
REGISTRATION MAIL GUIDE NOTE
REQUEST MAIL TEXT
SEND MAIL TEXT REQUESTED
RECEIVER'S MAIL SERVER
TITLE OF MAIL
REGISTRATION MAIL RECEPTION LINK
RECEIVER

Fig.5


SENDER
RECEPTION CONFIRMATION SIGNAL
MAIL
<MAIL CENTER>
MAIL SERVER
MAIL CONTROL SYSTEM(A)
DB
WEB SERVER
MAIL CONTROL SYSTEM(B)
REPLY
SEND MAIL TEXT REQUESTED
TITLE OF MAIL
REGISTRATION MAIL RECEPTION LINK
REGISTRATION MAIL GUIDE NOTE
REGISTRATION MAIL RECEPTION LINK
REGISTRATION MAIL GUIDE NOTE
TITLE OF MAIL
RECEIVER'S MAIL SERVER
RECEIVER

REGISTRATION MAIL SYSTEM WITH A SENT E-MAIL CHECK FUNCTION ON INTERNET AND METHOD FOR THE SAME

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a mail system and method for solving the problem that a sender cannot check whether or not a receiver received (read) a mail in an internet environment (FIG. **2**) that is a switching system among mail servers independently operated .

2. Description of Related Art

Existing PC communication services (e.g., Chollian, Hitel, Nownuri, and Unitel in Korea) each provides a sent e-mail check function in exchanging mail between its own service users. This is possible because the service is a single mail system. However, the mail exchange between users of different services cannot be achieved. Namely, messages can be exchanged by e-mail only between users registered in the same service (FIG. **1**).

On the other hand, users can freely exchange their message by e-mail regardless of services in which they registered according to the mail exchange system in the internet environment. Therefore, the existing PC communication services tend to provide an internet mail service together and the communication tends to be used based upon internet mail IDs (e-mail addresses). However, the existing internet mail service cannot provide a function allowing a sender to check whether or not a receiver read the mail sent by the sender. This is because internet mails are exchanged between independent mail servers. In this system, the sender cannot check the mail that the sender has sent to the receiver's mail server (FIG. **2**).

SUMMARY OF THE INVENTION

Accordingly, the present invention is directed to a registration mail system with a sent e-mail check function on internet and method for the same that substantially obviates one or more of the limitations and disadvantages of the related art.

An objective of the present invention is to provide a registration mail system with a sent e-mail check function, wherein a unique code is given to each mail sent by a sender and recorded in a database (DB), a common gate interface (CGI) executive program through which the unique code and confirmation information are sent to a source mail system if a receiver reads the mail is attached to the mail itself which is sent to the receiver's mail server, if the receiver reads the mail, the unique code and confirmation information that have been sent to the mail center by the CGI executive program are compared with database information and recorded in the database, and confirmation of reception by the receiver is notified to the sender.

Additional features and advantages of the invention will be set forth in the following description, and in part will be apparent from the description, or may be learned by practice of the invention. The objectives and other advantages of the invention will be realized and attained by the structure as illustrated in the written description and claims hereof, as well as the appended drawings.

To achieve these and other advantages, and in accordance with the purpose of the present invention as embodied and broadly described, the present invention employs a mail control system for assigning a unique code to a mail sent by a sender, recording the code in a database, and attaching a CGI executive program to the mail. The mail control system organically acts with a mail server and is in linkage with a database.

The present invention also employs another mail control system for comparing reception confirmation information from a receiver with database information, recording the confirmation information in the database, and sending an informing signal to the sender. This mail control system organically acts with a web server and is in linkage with the database.

When the receiver reads the mail in an off-line state, if a mail client application used by the receiver for reading the mail does not support a hypertext markup language (HTML), or if a text based emulator is used for reading the mail, the above system cannot be applied, so a registration mail system is developed as an extended type based upon the above system. In stead of using the program attached to the mail to process the reception confirmation information, the registration mail system stores the text of the mail therein and first sends only the information of a title of the mail, registration mail reception link, and registration mail guide note to the receiver. If the receiver requests the text of the mail, the registration mail system sends the text of the mail to the receiver and records the reception of the mail in the database.

It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are intended to provide further explanation of the invention as claimed.

BRIEF DESCRIPTION OF THE ATTACHED DRAWINGS

The accompanying drawings, which are included to provide a further understanding of the invention and are incorporated in and constitute a part of this specification, illustrate embodiments of the invention and together with the description serve to explain the principles of the invention.

In the drawings:

FIG. **1** is a block diagram showing a conventional mail system in PC communication;

FIG. **2** is a block diagram showing a conventional e-mail system in an internet environment;

FIG. **3** is a block diagram showing an overall structure of a mail system with a sent e-mail check function according to the present invention;

FIG. **4** is a block diagram showing an overall structure of an embodiment of a registration mail system with an extended sent e-mail check function according to the present invention; and

FIG. **5** is a block diagram showing an overall structure of another embodiment of a registration mail system with an extended sent e-mail check function according to the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

With reference to the accompanying drawings, the present invention will be described in detail.

FIG. **3** is a block diagram showing an overall structure of a mail system with a sent e-mail check function. Once a user composes a mail message and send it through this system, the mail is processed by a mail control system A which organically acts with a mail server. At this time, a unique code is assigned to the mail and the related information is recorded in a database. The mail control system A attaches the unique code and CGI executive program to the mail before sending it to the mail server of a receiver. If the

receiver reads the arrived mail, the CGI executive program is carried out so as to send information confirming the read of the message by the receiver and the unique code of the mail to a mail control system B in a mail center. The received mail code is compared with the mail codes previously recorded in the database to find the same mail code. Reception confirmation information is added to the corresponding mail record in the database. Thereafter, the mail control system B sends a reception confirmation signal to the sender. Furthermore, the sender can check the sent mail after accessing the web server anytime when necessary (FIG. **3**).

A registration mail system extended from the above system is similar to the above system in that a unique code is assigned to a mail sent by a sender. However, differently from the above system, the text of the mail is separately stored and a registration mail reception link and a registration mail guide note (indicates registration mail receive method for a user checking e-mail with an emulator based upon text) are attached to the mail in the mail center before sending the mail to the receiver's mail server. Once the receiver receives (reads) the mail, the text of the mail stored is requested through the registration mail reception link attached to the mail. The mail text is then received by the receiver through direct connection. At this time, the mail control system B compares the unique code of the mail with the mail codes in the database and adds reception confirmation information to the record of the corresponding mail in the database. Subsequently, the mail control system B sends the reception confirmation signal to the sender. Furthermore, the sender can check the sent mail after accessing the web server anytime when necessary (FIG. **4**).

However, if a mail client application used by the receiver for checking e-mail does not support HTML, or if the receiver checks the e-mail using the text based emulator, the above system cannot be applied. In this occasion, once the receiver just replies according to the content of the registration mail guide note, the mail control system A requests the text of the mail stored in the DB and sends it to the receiver. The mail control system A compares the unique code of the mail with the mail codes recorded in the DB and adds the reception confirmation information to the record of the corresponding mail. Thereafter, the mail control system B sends the reception confirmation signal to the sender. Furthermore, the sender can check the sent mail after accessing the web server anytime when necessary (FIG. **5**).

Consequently, the present invention makes it possible to use a sent mail check function on internet, thereby overcoming the defect of the internet e-mail that has been the main method for mail exchange.

As illustrated, the present invention embodies an internet mail system supporting a sent mail check function. This is sufficiently important to the part of e-mail as means of communication. For example, when the e-mail is used for business, there may be some cases the success of the business depends on whether or not the receiver reads within a certain time limit. There may be some cases that reception itself is refused or that a sender cannot check whether or not the receiver reads the mail by phone or other means. The sent mail check function is very important to the sender in these cases as well as daily mail exchange. In case a receiver uses a plurality of e-mail addresses, the present invention makes it possible for a sender to find and send e-mail to the receiver's e-mail address that is not used frequently. As illustrated, the sent mail check function is very useful. As internet e-mail becomes more important and necessary as means of communication, effect of the sent mail check function achieved by the present invention increases.

It will be apparent to those skilled in the art that various modifications and variations can be made in the registration mail system with a sent e-mail check function on internet and method for the same of the present invention without deviating from the spirit or scope of the invention. Thus, it is intended that the present invention covers the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. An electronic mailing method on the Internet with a function of reception confirmation comprising:

(a) assigning a unique code to an e-mail of a sender and recording in a database the information on the unique code assigned to the e-mail;

(b) attaching to the e-mail, to which the unique code was assigned in the step of (a), a CGI (common gateway interface) executive program that automatically sends to the web server of the sender the unique code that was assigned in the step (a) when the receiver receives the e-mail;

(c) sending the unique code of the received e-mail to the web server of the sender by the automatic execution of the CGI executive program when the e-mail, to which the unique code was assigned in the step of (a) and to which the CGI executive program was attached in the step of (b), is received by the receiver; and

(d) comparing the unique code of e-mail that was sent in the step (c) and the unique code that was recorded in the step (a) and, if they are identical, sending reception confirmation information to the sender.

2. An electronic mailing method on the Internet with a function of receipt confirmation, comprising the steps of:

(a) assigning a unique code to an e-mail sent by a sender and storing the unique code in a database;

(b) attaching a CGI executive program to the e-mail containing the unique code of step (a) in order to transmit the unique code which is assigned to the e-mail in step (a), to an e-mail system of the sender upon a receiver's receipt of the e-mail;

(c) transmitting the unique code of the e-mail received by the receiver to the e-mail mail system of the sender by an automatic execution of the CGI executive program upon the receiver's receipt of the e-mail which contains the unique code and the CGI executive program of step (b); and

(d) delivering receipt confirmation information to the sender of the e-mail if the unique code of the e-mail transmitted in step (c) is identical to the information stored in the database.

3. An electronic mailing system on the Internet with a function of receipt confirmation, comprising:

a first mail control system having a mail processor part which assigns a unique code to e-mail sent by a sender, attaches a CGI executive program for e-mail transmitting the assigned unique code to the electronic mailing system upon a receiver's receipt of the e-mail, and transmits the e-mail to the receiver's mail server;

a database in which the unique code assigned by the mail processor part is recorded; and

a second mail control system having a receipt confirmation part which receives the unique code of the e-mail transmitted by automatic execution of the CGI executive program, compares the transmitted unique code with the unique code recorded in the database, and transmits receipt confirmation information to the sender if the two unique codes are identical.

* * * * *

US006618747B1

(12) **United States Patent**
Flynn et al.

(10) **Patent No.: US 6,618,747 B1**
(45) **Date of Patent: Sep. 9, 2003**

(54) **ELECTRONIC COMMUNICATION DELIVERY CONFIRMATION AND VERIFICATION SYSTEM**

(76) Inventors: **Francis H. Flynn**, 14 Wave Crest Dr., Islip, NY (US) 11751; **Jeffrey Foran**, 1127 Commonwealth Ave., Apt. 1, Allston, MA (US) 02134

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/448,365**

(22) Filed: **Nov. 23, 1999**

Related U.S. Application Data

(60) Provisional application No. 60/109,934, filed on Nov. 25, 1998.

(51) **Int. Cl.**[7] **G06F 15/16**
(52) **U.S. Cl.** **709/206**; 709/203
(58) **Field of Search** 709/203, 206, 709/217; 345/744, 752; 379/93.24

(56) **References Cited**

U.S. PATENT DOCUMENTS

RE34,954 E		5/1995	Haber et al.	
5,426,594 A	*	6/1995	Wright et al.	709/206
5,509,071 A		4/1996	Petrie, Jr. et al.	
5,675,733 A		10/1997	Williams	
5,748,738 A		5/1998	Bisbee et al.	
5,771,355 A	*	6/1998	Kuzma	709/232
5,793,972 A	*	8/1998	Shane	709/219
5,850,520 A		12/1998	Griebenow et al.	
5,903,723 A		5/1999	Beck et al.	
5,930,471 A	*	7/1999	Milewski et al.	709/204
6,018,774 A		1/2000	Mayle et al.	
6,275,848 B1	*	8/2001	Arnold	709/206
6,332,164 B1	*	12/2001	Jain	709/235
6,385,655 B1	*	5/2002	Smith et al.	709/232
6,477,243 B1	*	11/2002	Choksi et al.	379/100.06

FOREIGN PATENT DOCUMENTS

WO WO 02/25508 A2 * 3/2002

OTHER PUBLICATIONS

Gralla, P., How the Intranets Work, Ziff–Davis Press, pp. xi & 122–125, 1996.*

Stallings, W., Data and Computer Communications, Prentice–Hall, pp. 728–730, 1997.*

Lowe, D., Client/Server Computing for Dummies, IDG Books Worldwide, pp. 125–128 and 136–137, 1995.*

Gralla, P., How the Internet Works, Special Edition, Ziff–Davis Press, pp. 76–86, 110–111 and 122–125.*

Microsoft Press Computer Dictionary, 3rd ed., Microsoft Press, pp. 34–35, 1997.*

Klensin et al; Request for Comments: RFC 1869 (Nov. 1995) available at http://www.gssnet.com/rfc/rfc1869.htm, pp. 1–11.

Freed; Request for Comments: RFC 2034 (Oct. 1996) available at http://www.gssnet.com/rfc/rfc2034.htm, pp. 1–5.

Mosher, Sue; Microsoft Exchange User's Handbook; Duke Press (1997); pp. 220, 285, 288.

Blue Mountain Arts. Frequently Asked Questions. www-.bluemountain.com/help/FAQ2.html, pp. 5–6 & 11.

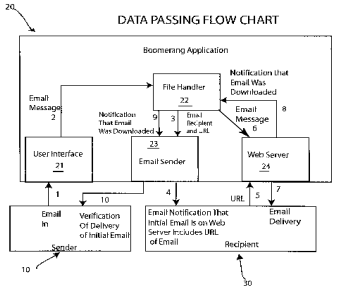
* cited by examiner

Primary Examiner—Andrew Caldwell
(74) *Attorney, Agent, or Firm*—Collard & Roe PC

(57) **ABSTRACT**

The present invention provides a system and a method for a user to verify receipt of an electronic communication such as an email message by an intended recipient. Instead of forwarding the email to the intended recipient(s), (e.g. as a normal SMTP server might,) the invention sends a notification message of a posted email to the intended recipient(s). The email and attachments are each saved at a unique call address on a server such as for example a web server. At least one unique address is provided for each of the intended recipients that points to the location of the contents of the original email. When attachments accompany the email, each attachment is also assigned an address that is unique for each intended recipient. The intended recipient is notified of the call addresses for collecting the email and attachments. When the recipient downloads or collects the email and attachments from their respective addresses, the invention detects information regarding the downloaded email and notifies the sender that the email was retrieved. This information may be stored in a back-end database for ease of access and management.

6 Claims, 2 Drawing Sheets



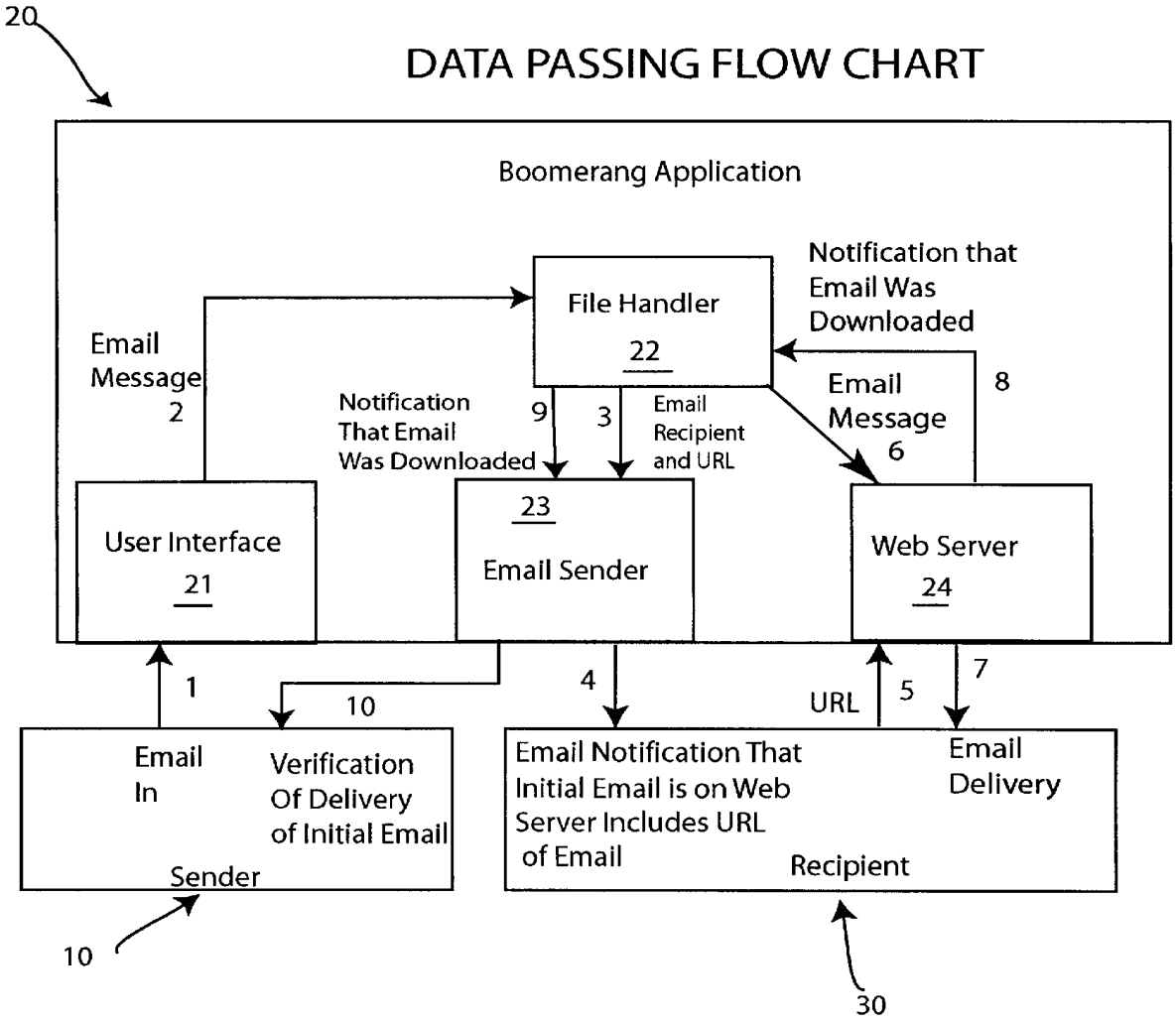
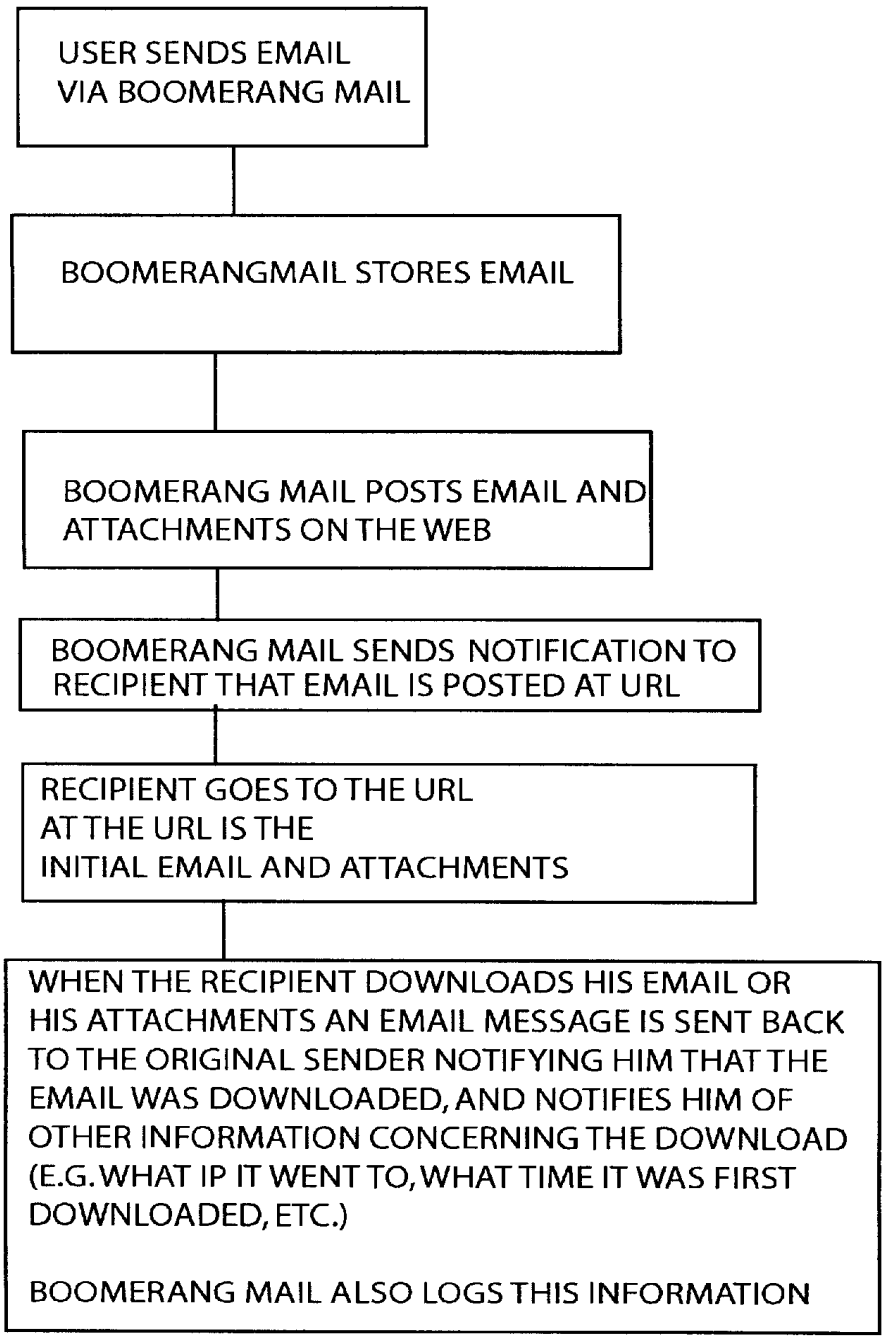

20
DATA PASSING FLOW CHART
Boomerang Application
File Handler
22
Notification that
Email Was
Downloaded
Email
Message
2
Notification
That Email
Was Downloaded
9
3
Email
Recipient
and URL
Email
Message
6
8
User Interface
21
23
Email Sender
Web Server
24
1
10
4
URL
5
7
Email
In
Verification
Of Delivery
of Initial Email
Sender
Email Notification That
Initial Email is on Web
Server Includes URL
of Email
Email
Delivery
Recipient
10
30

FIG. 1

FIG. 2

SEQUENCE OF STEPS TAKEN DURING BOOMERANG MAIL USE



ELECTRONIC COMMUNICATION DELIVERY CONFIRMATION AND VERIFICATION SYSTEM

This application claims the benefit of U.S. Provisional Patent Application 60/109,934 filed Nov. 25, 1998, entitled "An Electronic Communication Delivery Verification System", the content of which is incorporated herein by reference in its entirety.

FIELD OF THE INVENTION

This invention relates generally to electronic communications and, more particularly, to a method by which a sender of an electronic communication can validate receipt of an electronic communication by an intended receiver.

BACKGROUND OF INVENTION

Electronic communication, such as for example e-mail, is a form of written data, a data-string, that is transported electronically such as on the Internet. Specific protocols governing certain aspects of the way one machine electronically passes information in the form of data-strings to another machine have been established to facilitate communication between different brands of machines running different software. Various protocols have been developed to standardize the methods by which data are transported from one computer to another computer such as on Local Area Networks (LAN), Wide Area Networks (WAN), and the Internet. This standardization was developed to allow computers and computer programs from differing commercial sources to be as compatible as possible.

The Internet Protocol (IP) that directs or routes a data-string from one computer to another is what is called a best efforts protocol, a method that involves a series of computer instructions that attempts to deliver a data-string to its intended location, but that does not guarantee its delivery. This means that the data-string can get lost or damaged before reaching the intended recipient. The Transmission Control Protocol (TCP) works in conjunction with IP in an attempt to ensure that data-string is sent error-free, complete, and in the proper sequence. However, it does not insure correct delivery. The Simple Mail Transfer Protocol (SMTP) provides for standardized error messages to be issued when a fault occurs in transmission. Standardized status codes (such as described in Kleinsin, et al; Network Working Group Request for Comments: 1869; STD: 10: Obsoletes: 1651; Category: Standards Track; November, 1995) provide information for generating error messages that indicate whether or not a computer in the net or network of computers used to pass the data-string has been unable to do so. Such an Error message is exemplified by:

"----The following addresses had delivery problems ----
<nosuchuser@dbc.mtview.ca.us>
(Mailbox "nosuchuser" does not exist)"

When delivery occurs a message such as "---Mail was successfully relayed to the following addresses---" may be provided. However, no information is provided by through the use of these protocols via the respective protocol server regarding whether the intended recipient has retrieved the email and/or the attachments.

Business people and others need to verify that an important transaction once sent has been received by the intended recipient. The main obstacle to widespread commercial use of electronic communications, such as for example email and email attachment, is the lack of the ability to verify that the email and/or attachment was received by the intended recipient. Email must be sent on unsecured pathways, pathways where the email can be mis-directed, lost, and/or altered. It is highly desirable to the sender to be able to verify that the intended recipient has received an important email. It is also desirable to the sender to know that the intended information in electronic message was received as written or sent.

SUMMARY OF INVENTION

The instant invention comprises a software application for use with a computer that is part of or has access to an electronic network including at least one other computer and a method for use of the software application that provides a sender of an electronic communication such as an email, a receipt for verification of delivery of the electronic communication by a recipient. The sender may use a conventional email program or the instant invention to compose the email. The email ("electronic mail") may have graphics and/or attachments, each of which is termed a data-string herein. Unlike a conventional email program, each data-string is directed to a unique electronic address, such as for example an IP (Internet Protocol) address or hostname, on a computer that is independent of the recipient's computer. Only a notification that an email or an email plus an attachment is awaiting retrieval is sent to the recipient and appears at their computer. The notification provides the recipient with the unique electronic retrieval location(s), such as a unique IP address for an email message or two unique email addresses for an email accompanied by an attachment, located on a mail server to which the recipient can direct their computer using software to retrieve the data-string(s). Each recipient is provided with a unique address to retrieve their email even when the recipient is merely receiving a copy of an email that has been broadcast to a number of recipients. In one embodiment, a computer having access to the Internet is used as the mail server. In an alternate embodiment, the mail server is located on a LAN (local area network) such as for example for use for infra-office email within a business. Upon retrieval of the data-string, the sender is notified electronically via email and information regarding the retrieval transaction is stored in a back-end database.

For example, when the data-string is sent via the Internet, the user who is the sender composes an email message and attaches any text or images as required. Once the message is composed and sent, the instant invention parses that data-string while determining the appropriate recipients. The parsed data-string is placed on the World Wide Web (also termed the Web or the Internet or the Net) by waiting until at least one appropriate data-string transfer and retrieval means, such as for example a HyperText Transport Protocol (http) call provides an available address at a port of a computer the instant invention is monitoring. More addresses will be needed to match data-string to address when, for example, a single email data-string is being communicated to a number of different recipients. There is exactly one unique address that will access the data-string for each specific recipient targeted to receive the data-string unless the data-string has more than one component such as a plurality of attachments. Concurrent with posting the sender's data-string on a computer connected to a network of computers such as the Web, the instant invention sends out a notice via email that the recipient has a posted data-string or email awaiting retrieval. This message is simply a notice of the availability of the electronic communication that provides an electronic address such as a Uniform Resource Locator (URL) pointer to where the email is posted on the Web. One URL points to a single location that

is uniquely assigned for each component of the data-string for each recipient using the instant invention. Alternatively, the posted email may have a URL that allows it to call for its accompanying attachment ie. the email and its accompanying documents may be electronically interlinked.

When the recipient of the email message links to a data-string via the URL pointer, the instant invention identifies the recipient by their unique IP address or hostname. As the recipient retrieves their posted email message and attachments, the instant invention notifies the sender that the posted electronic communication has been retrieved by a person at the IP address corresponding to that of the intended recipient. This notice includes the recipient's unique IP address or hostname and a time, date stamp indicative of when the posted electronic communication was retrieved. A copy of the posted electronic communication may also be included in the notice.

An embodiment of an inventive method for verifying receipt of an electronic communication at an intended electronic address is provided by the following example comprising the steps of:

1. Sending an electronic communication comprising a data-string.
2. Posting that data-string to a unique URL on a computer connected to the Web for each unique data-string.
3. Notifying the recipient at a recipient IP address via email that they have an electronic communication awaiting retrieval at a specified unique Web URL address.
4. Validating the retrieval of the sender's electronic communication by a recipient at an intended IP address by recognizing the recipient's IP address or hostname when they electronically request delivery of their electronic communication.
5. Notifying the sender when the IP address or hostname match the intended IP address or hostname that the electronic communication has been retrieved and optionally passing the validating information into a back-end database.

The invention has four distinct interfaces with users: two sender interfaces and two recipient interfaces. The first sender interface is an outgoing message interface that is implemented to communicate with any SMTP client having an outgoing server that is configurable to a given IP address or hostname. This interface is not limited to what is generally considered client type programs such as for example email programs such as Eudora®. The invention could interface at the first sender interface with any large server that delivers email using SMTP where the outgoing delivery IP address is capable of being configured. The first recipient interface is implemented to accommodate use with any system or application that handles delivery of electronic messages to a given recipient. This includes all POP clients, all Web-based email clients as well as any test-based email delivery and retrieval systems. The second part of the recipient interface is the data-string retrieval interface. This interface is implemented to communicate only via http (with any http browser in the embodiments described. However, the recipient interface can be implemented to accommodate any data-string retrieval mechanism. The second sender interface is the incoming interface that notifies the sender when the data-string is retrieved. In one embodiment, it is implemented as an email delivery notification and works with any system that handles delivery of email to a given recipient. This includes all POP clients, all Web based clients, as well as any text-based email retrieval systems.

In one embodiment, the instant invention communicates (also termed "interfaces") with electronic communications program, such as for example email programs Eudora®, First Class Client®, and Hot Mail®. It can be used for electronic communication on the Internet or an Intranet, within a Local Area Network (LAN) or a Wide Area Network (WAN) environment. The invention provides a plurality of fields for data in the back-end database. Full search, browse, edit, and contact management functions are included in order to provide complete access to the stored data. Remote access functions may be configured. Thus, verification, authentication, and ease of data management are provided. Advantageously, the flow of electronic communications such as email can be controlled and documented.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** provides a block diagram of the system and method by which an electronic communication in the form of data can be routed by a sender to a specific receiver and by which the sender can be notified of the receipt of the electronic communication by the specific receiver.

FIG. **2** provides a flow chart of the pathway and components used to transmit and verify an electronic communication.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The instant invention provides a system and method for confirmation of receipt of an electronic communication by an IP address or hostname accessible recipient ("the recipient"). The invention is a software application that allows the sender of an electronic communication to use the electronic communication program of their choice, such as for example an email program like Eudora®, to generate a specific data-string or message, send it to a specific recipient, and verify that the specific recipient received the data-string. Optionally, the application may provide a copy of the retrieved data-string so that the sender can determine if the data-string was received as sent, unaltered. Transmission of electronic information involves passing data in the form of a data-string from one computer to another through the use of computer programs that convert user instructions into instructions that a computer can understand. The data-string is then passed through electronic means, such as for example by telephone wires or cables, from one computer to another computer. These computers form a network of computers that is variously referenced to as a "Net" or "Web".

The invention has four distinct interfaces with users: two sender interfaces and two recipient interfaces. The first sender interface is an outgoing message interface that is implemented to communicate with any SMTP client having an outgoing server that is configurable to a given IP address or hostname. This interface is not limited to what is generally considered client type programs such as for example email programs such as Eudora®. The invention could interface at the first sender interface with any large server that delivers email using SMTP where the outgoing delivery IP address is capable of being configured. The first recipient interface is implemented to accommodate use with any system or application that handles delivery of electronic messages to a given recipient. This includes all POP clients, all Web-based email clients as well as any test-based email delivery and retrieval systems. The second part of the recipient interface is the data-string retrieval interface. This

interface is implemented to communicate only via http (with any http browser in the embodiments described. However, the recipient interface can be implemented to accommodate any data-string retrieval mechanism. The second sender interface is the incoming interface that notifies the sender when the data-string is retrieved. In one embodiment, it is implemented as an email delivery notification and works with any system that handles delivery of email to a given recipient. This includes all POP clients, all Web based clients, as well as any text-based email retrieval systems.

Referring now to FIG. **1** which illustrates a first embodiment of the instant invention, when an electronic communication sender is distanced from a recipient and the Internet is used to send the electronic communication, a sender illustrated by box "Sender" **10** enters information, such as for example an email message and an attachment to that email message, into a computer via the desired electronic communications program that has been loaded on that sender's machine. A message data-string is generated. This message data-string is then processed by the instant invention which has been loaded on the sender's machine as follows. The message data-string is parsed into an html-readable file and electronically sent via a user interface **21** to a file handler **22** where the message data-string is stored at a unique http call address assigned to each of the intended recipients. Assignment of the unique http call address(es) is determined by the instant invention which monitors a port for incoming TCP connections. If the electronic communication was an email that included an attachment, then a unique address is assigned to each of the parsed original email message and original attachment html-readable files. Concurrently upon receiving a file for storage, the file handler also generates a unique data-string for each stored file that is a notification message that is delivered to each unique recipient. This notification data-string informs each recipient that one unique message data-string has been stored for them at the indicated unique http call address. This notification data-string is sent via a Web Server **24** to the intended unique recipient, represented by box "recipient" **30**.

The notification data-string may have additional information added to it prior to its delivery to the recipient. For example, the electronic communication sender's name and/or email address may be added. Or, an advertisement may be added to the notification message data-string.

The notification message data-string is then sent to the recipient's Post Office Protocol (POP) server and is read by the recipient at the notified IP address or hostname address indicated by the notification message when they open their email application. If the recipient wishes to read the posted electronic communication, the recipient enters the unique http call address that has been sent in the notification message data-string and retrieves the unique message data-string from the Web Server **24**, if the recipient has entered the correct http call address. Both an email and its associated attachment(s) can be provided with unique call addresses or the email and its attachment(s) can be linked so that the entire communication is available using one call address. In a first embodiment for each stored message data-string retrieved, be it email or attachment, the Web server sends a notification of receipt message that informs the sender that the message data-string was retrieved by the recipient at the address receiving the notification of available email and http call address. This notification of receipt message is electronically transmitted to the sender at approximately the same time that the recipient is sent (retrieves) the stored message data-string. The notification of receipt message is sent via the file handler and the email sender to the IP or hostname address of the sender ("original sender") and includes information concerning the downloading of the message data-string by the recipient, such as for example, the time it was first downloaded (time and date stamp), the address to which it was sent at downloading, and other relevant information. A compressed copy of the message received by the recipient may also be provided to the sender.

If the original electronic communication comprises an email and an attachment, then in one embodiment, the recipient is notified that an electronic communication is located at http call address **1** (the email) and at http call address **2** (the attachment). The recipient retrieves the electronic communications at each address and notification of each separate retrieval is provided to the sender as described above. Alternatively, the notification message may contain a link to the address for the email and to the address for the attachment. Notification of receipt may then be sent as each data-string is retrieved or notification of receipt may be sent only once when all associated electronic communications have been retrieved.

FIG. **2** provides an embodiment of a method of confirming that an electronic communication was received by a recipient. This embodiment exemplifies electronic communication verification when using the Internet to transport the electronic communication. Referring now to FIG. **2**, a flowchart of the steps used to provide verification to a sender that receipt of a electronic communication by a recipient has occurred is provided. The sender installs the software, the inventive computer program for generating electronic mail receipts, on their computer and electronically moves through a set-up interface. The sender generates an electronic communication such as an email. The sender enters the email address of the intended recipient or recipients thus providing an addressed packet of information or a message data-string which includes the address of the intended recipient that is unique for each intended recipient. The message data-string is converted to html-readable language and passed to a file handler via a user interface. The message data-string is stored while the instant invention locates one unoccupied call address, such as for example an http call address, if the message data-string is going to only one recipient. Otherwise, the instant invention recognizes that a plurality of unique call address are required and establishes one unique call address for storage of each copy of the email sent to the plurality of intended recipients. In the simplest case where there is one recipient, the message data-string is then posted to this unique unoccupied call address which is on a Web server. Concurrently, a notice that the recipient has email from the sender on the Web server at the call address at which the message data-string is located is sent to the recipient's Post Office Protocol (POP) server, notifying the recipient that they have an electronic communication. The recipient requests the message data-string located at the provided unique call address and it is sent to the recipient, who downloads it, opening it. Upon downloading of the message data-string, the instant invention generates a notice of receipt that is forwarded to the original sender. The notice of receipt forwarded to the sender at the sender's POP server includes information concerning the collection of the email by the recipient such as for example the address to which the email was downloaded, the time it was downloaded, and optionally, a compressed copy of the original message. When the sender enters their POP server, they receive the notification of receipt by the recipient.

When attachments accompany an email, each of the attachments and the email itself is provided with a unique

call address. Each is collected separately by the intended recipient. The intended recipient may be notified of each separately or the intended recipient may be directed to the email call address which then provides the recipient with the unique call addresses of each of the attachments.

Notification of receipt of the email and attachments can be achieved in a variety of ways and may vary depending upon the number of recipients and the number of attachments sent. Notification can be sent as each unique recipient accesses each unique call address. Or, notification may be sent to the sender when the recipient has collected the email and all of its associated attachments. Or, where a plurality of recipients have been sent the same email, the sender may be notified only after all the recipients have retrieved their copies of the email. Preferably, in the notification of receipt, a copy of the electronic message as received by the recipient is included. This message may then be compared with the message sent to verify that the message was not garbled during transmission. Other options will be apparent to those skilled in the art.

The instant invention also may be inactivated without having to remove the software application off the computer hard disc. The instant software application is provided with the following switches: Override, Always On, and Switch. Override allows the user to substantially turn off the software application thus deactivating notification of receipt. "Always On" allows the user to send electronic communication which provides notification of receipt whenever the electronic communication is accessed. Switch provides a subroutine that reads the electronic communication before its is sent by the sender to determine if a receipt is being requested.

Modifications and variations can be made to the disclosed embodiments without departing from the subject and spirit of the invention as defined in the following claims. Such modifications and variations, as included within the scope of these claims, are meant to be considered part of the invention as described.

What is claimed is:

1. A method for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) posting said data-string having said electronic address to a unique call address;

c) providing the intended recipient with said unique call address at said electronic address;

d) receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data string;

e) comparing said electronic address in said request with said electronic address provided in said data-string and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said data-string;

f) sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

2. The method as in claim **1**, further comprising the step of posting said data in a back end database.

3. A method for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) sending an attachment to said electronic communication to an additional electronic address for the intended recipient;

c) posting said data-string having said electronic address to a unique call address;

d) posting said attachment having said additional electronic address to an additional unique call address;

e) providing the intended recipient with said unique call address at said electronic address;

f) receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data-string;

g) comparing said electronic address in said request with said electronic address provided in said data-string and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said data-string; and

h) sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

4. The method as in claim **3**, further comprising the step of posting said data in a back end database.

5. A device for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) means for sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) means for posting said data-string having said electronic address to a unique call address;

c) means for providing the intended recipient with said unique call address at said electronic address;

d) means for receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data string;

e) means for comparing said electronic address in said request with said electronic address provided in said datastring and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said datastring; and

f) means for sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

6. A device for verifying receipt by an intended recipient of an electronic communication generated by a sender comprising the following steps:

a) means for sending an electronic communication comprising a data-string having an electronic address for the intended recipient;

b) means for sending an attachment to said electronic communication to an additional electronic address for the intended recipient;

c) means for posting said data-string having said electronic address to a unique call address;

d) means for posting said attachment having said additional electronic address to an additional unique call address;

e) means for providing the intended recipient with said unique call address at said electronic address;

f) means for receiving at said call address a request, having said electronic address for the intended recipient therewith, to access said data-string;

g) means for comparing said electronic address in said request with said electronic address provided in said datastring and proceeding with accessing said data string when said electronic address in said request matches said electronic address in said datastring; and

h) means for sending an electronic notification consisting of data, said data comprising said call address and said electronic address of the intended recipient to the sender when said electronic communication is accessed by the intended recipient.

* * * * *

US006836846B1

(12) **United States Patent**
Kanevsky et al.

(10) **Patent No.: US 6,836,846 B1**
(45) **Date of Patent: Dec. 28, 2004**

(54) **METHOD AND APPARATUS FOR CONTROLLING E-MAIL ACCESS**

(75) Inventors: **Dimitri Kanevsky**, Ossining, NY (US); **Mariusz Sabath**, Scarsdale, NY (US); **Alexander Zlatsin**, Yorktown Heights, NY (US)

(73) Assignee: **International Business Machines Corporation**, Armonk, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/422,196**

(22) Filed: **Oct. 21, 1999**

(51) **Int. Cl.**[7] **H04L 9/32**
(52) **U.S. Cl.** **713/193**; 707/10; 707/9
(58) **Field of Search** 713/193, 201; 707/10, 9; 705/54

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,314,409 B2 * 11/2001 Schneck et al. 705/54
6,591,367 B1 * 7/2003 Kobata et al. 713/201

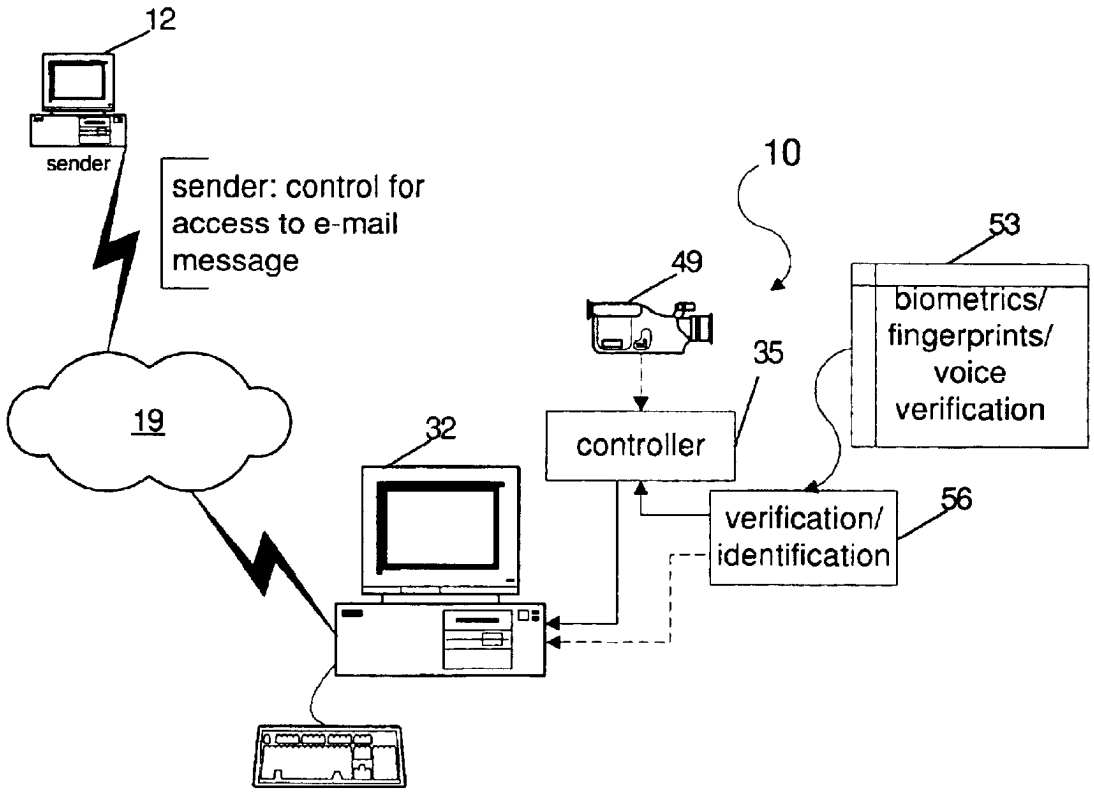
* cited by examiner

Primary Examiner—Steven Fischman
Assistant Examiner—Thanhnga Truong
(74) *Attorney, Agent, or Firm*—Scully, Scott, Murphy & Presser; Daniel P. Morris, Esq.

(57) **ABSTRACT**

A system for controlling access to electronic information packages including e-mail messages communicated from a sending device to a receiving device at one or more destination locations. The system and method includes determining fulfillment of one or more certain conditions at the destination location; and, implementing control in response to detection of a fulfilled one or more certain conditions to enable access to content provided in a communicated package. The access includes enabling a user to perform certain operations on the package content at the destination location, or, preventing certain operations from being performed. A mechanism is included for enabling automatic destruction of the e-mail messages immediately after being read by an authorized recipient, or, after a predetermined time interval from receipt of the message. A verification system is employed enabling a sender to verify users attempting to access the e-mail.

50 Claims, 4 Drawing Sheets



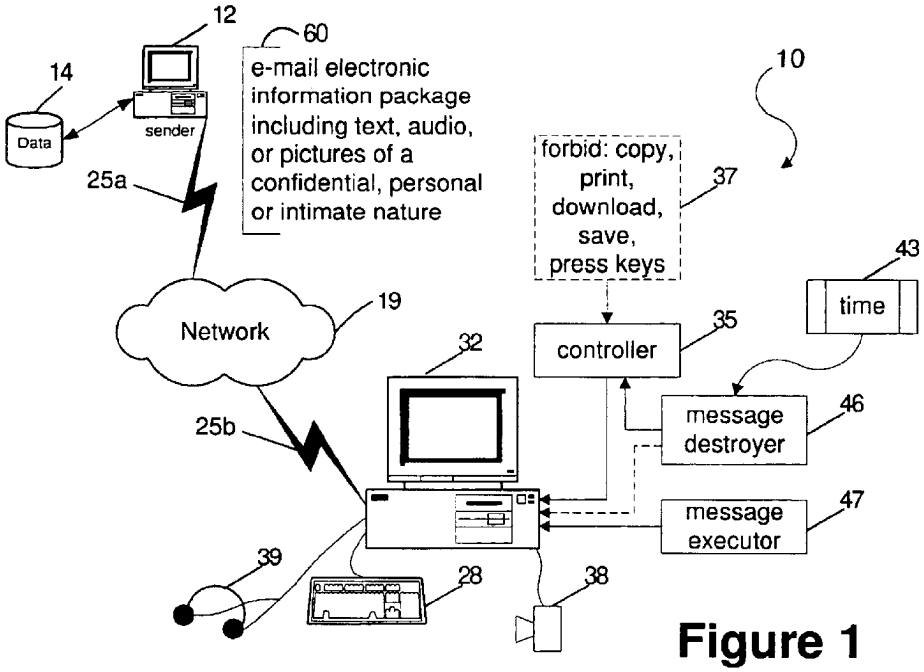


Figure 1

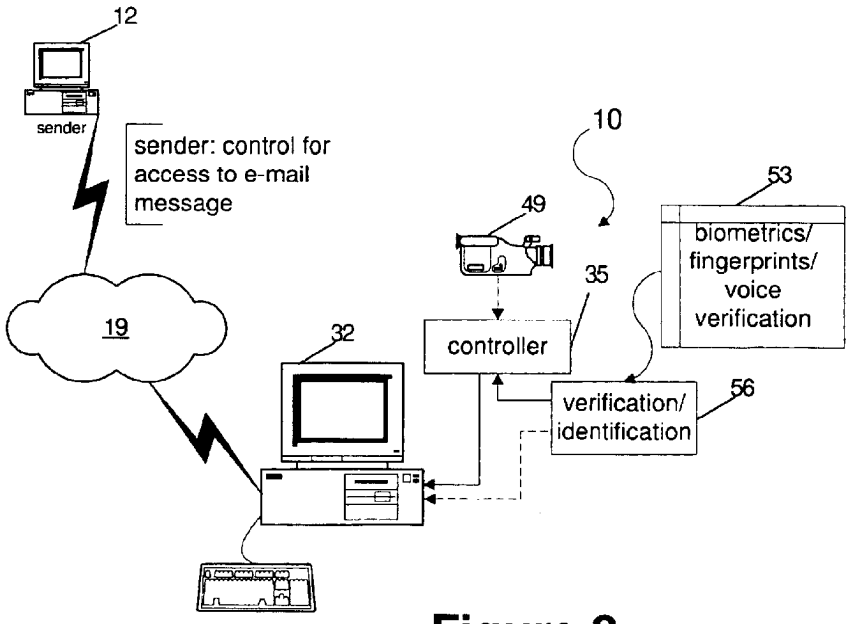


Figure 2

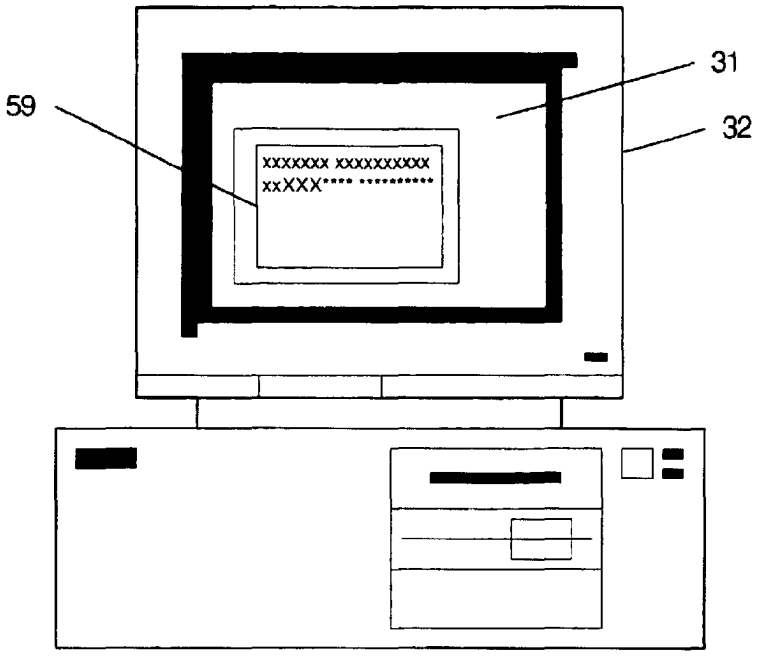


Figure 3

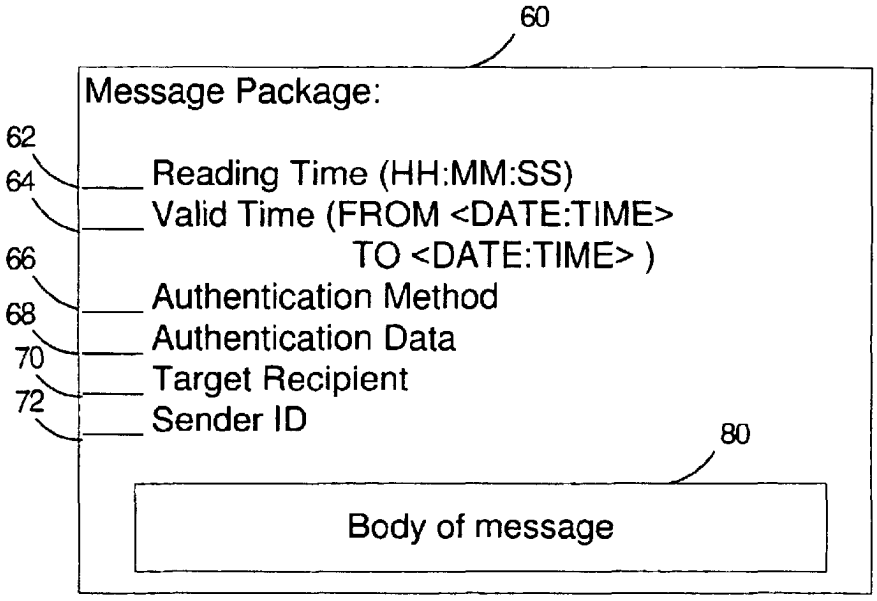


Figure 4

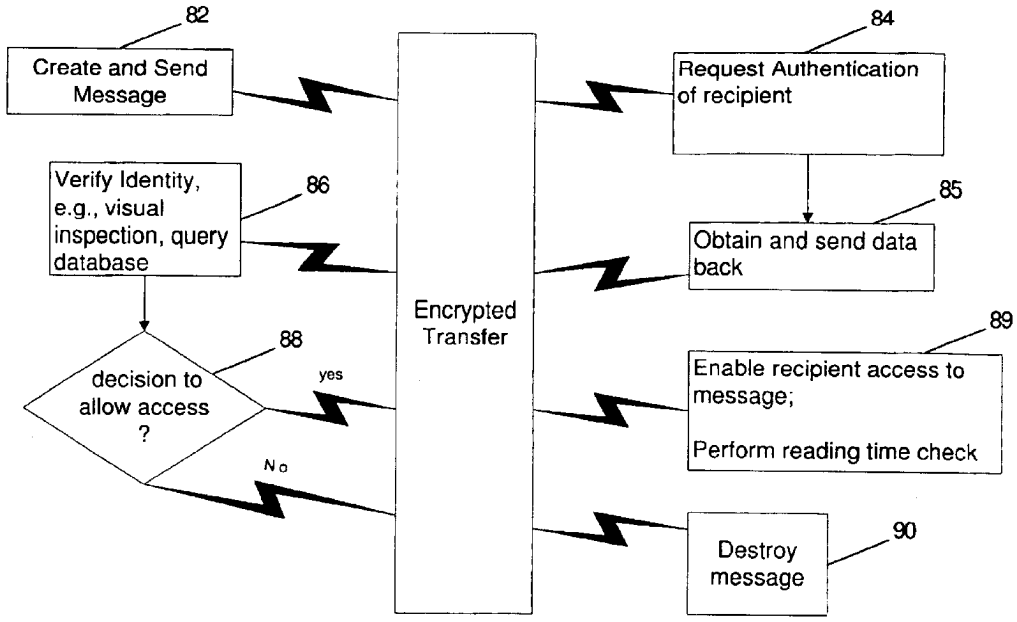


Figure 5(a)

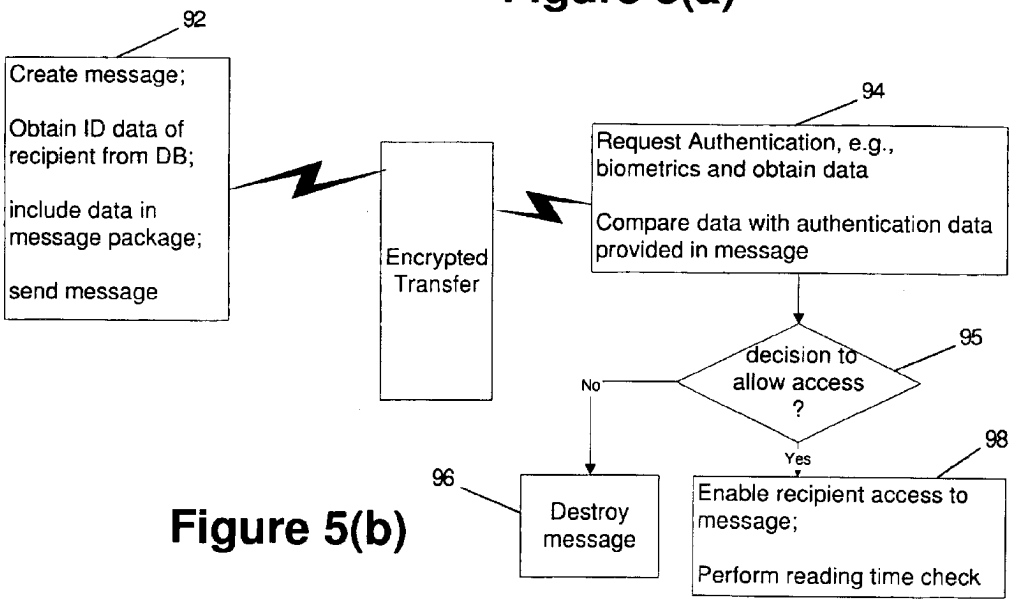


Figure 5(b)

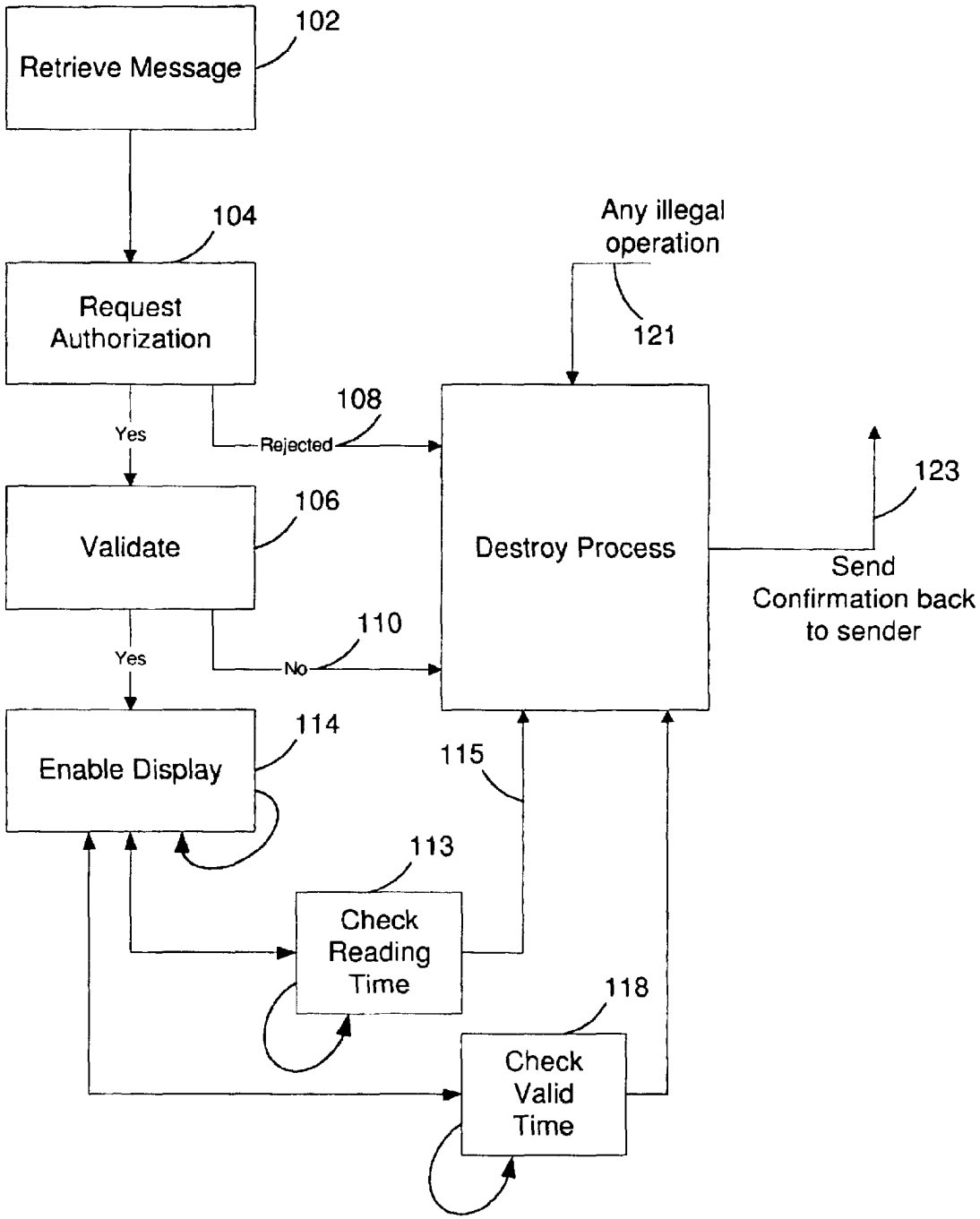

Retrieve Message
102
Request Authorization
104
Any illegal operation
121
Yes
Rejected
108
Validate
106
Destroy Process
123
Send Confirmation back to sender
Yes
No
110
Enable Display
114
115
113
Check Reading Time
118
Check Valid Time

Figure 6

METHOD AND APPARATUS FOR CONTROLLING E-MAIL ACCESS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to e-mail messaging systems, and, particularly, to a system and methodology for controlling access to e-mail data content present in e-mail messages.

2. Discussion of the Prior Art

Senders of E-mail messages often want the message to be retrieved and accessed by the intended recipient and not made available to anybody else to access. For example, a sender of an e-mail message including content of an intimate or personal nature would like to prevent a receiving user from showing his/her note to other people. Standard prevention methods that include encryption only helps to prevent unauthorized access to data while it is being communicated over the communication medium, e.g., phone lines. These security methods however, cannot prevent improper use of messages at a receiving end after they are decrypted.

It would thus be highly desirable to provide a system and method that enables a sender to control access to e-mail data after sending the e-mail message to the intended recipient.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a system and method for enabling a sender to control access to e-mail and electronic information content after sending the e-mail message to an intended recipient.

According to a preferred embodiment of the invention, there is provided a system and method for controlling access to electronic information packages including e-mail messages communicated from a sending device to a device at one or more destination locations. The system and method includes determining fulfillment of one or more conditions at the destination location; and, implementing controls in response to detection of a fulfilled one or more conditions to enable access to content provided in a communicated package. The access includes enabling a user to perform certain operations (e.g., playing, displaying) on the package content at the destination location, or, preventing certain operations from being performed (e.g., copying, saving). A mechanism is included for enabling automatic destruction of the e-mail messages immediately after being read by an authorized recipient, or, after a predetermined time interval from receipt of the message. A verification system is additionally employed enabling a sender to verify and authenticate users attempting to access the e-mail at the destination location prior to authorizing use or playback of the e-mail message.

BRIEF DESCRIPTION OF THE DRAWINGS

Further features, aspects and advantages of the apparatus and methods of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG. **1** is a general block diagram depicting the system for controlling e-mail access by senders.

FIG. **2** is a diagram illustrating how a sender controls access to his/her message at a receiving computer terminal.

FIG. **3** is an illustration depicting the window shell e-mail message according to the invention.

FIG. **4** is an illustration depicting the electronic information package to be sent by the sender.

FIG. **5**(*a*) is an illustration depicting the method implemented for remote authorization according to the invention.

FIG. **5**(*b*) is an illustration depicting the method implemented for local authorization according to the invention.

FIG. **6** is an illustration depicting the general workflow process performed at the receiver terminal.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. **1** is a general block diagram depicting the system **10** for controlling e-mail access by senders. As shown in FIG. **1**, the system implements electronic devices for sending one or several electronic information packages **60** from one or several computer devices **12** at originating locations through communication channels **25***a,b*, such as telephone channels, wireless channels, radio links for delivery over a network, e.g., the Internet **19**, to one or several computer devices **32** at destination locations. In the preferred embodiment, "electronic information packages" αinclude one or more of the following data types: e-mail messages, audio data, video data, animation data, textual data, pictorial data, which may include content of a confidential, personal, or intimate type. It is understood that an electronic information package may include any other types of data content, i.e., of a non-personal nature. According to the invention, the system enables access to these packages at the destination points and controls access to these packages at destination points by allowing or forbidding certain operations to be performed on these packages at these destination points in accordance with predetermined conditions. That is, only if certain predetermined conditions at these destination points are fulfilled, access to or destruction of these information packages is enabled.

It is understood that computer devices **12**, **32** at originating and destination locations are devices that comprise CPU and memory storage devices. (not shown) however, such devices **12**, **32** may include: laptop/notebook computers, embedded devices, and consumer electronics (kitchen appliances, TV, electronic gadgets, palmtops, and telephones). Further, as shown in FIG. **1**, the sending terminal will include a memory or database storage device **14** comprising recipient verification/authentication data accessible by the sender as will be described herein.

As shown in FIG. **1**, the computer device **32** at the destination location includes a modified e-mail program or executor **47** for retrieving and notifying a recipient of a retrieved message. The recipient computer device **32** further includes a controller module **35** implementing software controls for preventing certain operations **37** from being performed on received electronic information packages in accordance with the invention as discussed herein. Such controls include the satisfaction and/or determination of one or more certain conditions, as will be described in greater detail herein. Particularly, the controller module **35** permits or prevents one or more of the following operations to be performed on the received electronic information packages: a saving operation for saving these packages in memory storage devices at destination points; a transfer operation such as copying, printing, storing or downloading of these packages and data to memory storage devices; a displaying operation for video data, text, picture and animation data on one or several display devices (not shown) at destination points; and, playing audio data on one or several audio playback/speaker devices **38** at destination points (as shown in FIG. **1**). It is understood that other operations such as the destruction of the received electronic package may be

enabled or prevented by controller module **35**. Alternately, the electronic information package itself may be equipped with a program that is capable to control access to its content and destroy these packages when certain conditions are fulfilled. Thus, for instance, a sender system may be equipped with a program that is capable of controlling access to its content and destroy these packages when the certain conditions are fulfilled.

In a preferred embodiment, an electronic information package may be automatically destructed at the destination computer terminal **32** at a pre-determined time after it is received. Thus, as shown _in FIG. **1**, a message destroyer process **46** which may be executing as part of the controller module, or separately therefrom, implements a timer mechanism **43** for determining time elapsed from receipt of the electronic information package at computer device **32**. After one or more pre-determined time intervals has elapsed, the message destroyer mechanism **46** will automatically trigger a destruction operation in the computer terminal for deleting the electronic information package. According to the invention, the number of intervals and length of a time interval may be set by the sender of the message, for instance, as a parameter to be entered as part of the e-mail message. As will be described in greater detail herein, this parameter information is received as part of or, in addition to the e-mail message, and implemented by the message destroyer **46** and timer mechanisms at the destination device **32**. The actual destruction operation may be performed by the controller module **35** separately from or, in conjunction with a particular computer operating system.

It is understood that other conditions may be satisfied for triggering the destruction of a received electronic information package at the destination computer terminal. The other conditions include, but are not limited to the following: a) the detection of someone or something trying to perform a forbidden operation on the received electronic information package at the computer device **32**; b) the direct command from the e-mail sender to instruct the control module to destroy a message at a later point in time; c) the detection of a modification or change in the CPU; a change in memory amount, or memory modification; a modification to or change of a peripheral device implemented at computer devices at destination points that are not related to the process of displaying or playing information packages at destination points; and d) the detection of when a playback and/or display of information package content is completed at the destination computer device **32**.

Preferably, the condition a) of detecting attempted performance of a forbidden operation on the received electronic information package at the computer device **32** may be specified by the sender and entered as a parameter in the e-mail message, or, as a data attached to the message. As mentioned herein, types of forbidden operations include: a saving operation for saving these packages in memory storage devices at destination points; and, a transfer operation such as copying, printing, storing or downloading of these packages and data to memory storage devices. In operation, the control module **35** either separately from or, in conjunction with the computer device's operating system, will detect such a forbidden operation attempt, and trigger the destroyer process **46** to destruct the received electronic information package. Similarly, as for condition b) the sender may additionally send a direct command via e-mail at a later point in time as a parameter in the e-mail message, or, as data or a program attached to the message in order to trigger the destroyer process **46** to destruct the received electronic information package.

Preferably, the condition c) of detecting a modification or change in the CPU or a change/modification of memory or peripheral device may be specified by the sender of the package and performed by the control module **35**. Once such a condition is detected, the control module will trigger the destroyer process **46** to destruct the received electronic information package. Similarly, as for condition d) the control module **35** will trigger the destroyer process **46** to destruct the received electronic information package upon detection of a second or subsequent attempt to playback and/or display information package content at the computer device **32**.

Still other conditions may be satisfied for triggering the destruction of a received electronic information package at the destination computer terminal. As shown in FIG. **1**, the other conditions include, but are not limited to the following: e) the detection of one or several processes running in CPU or memory devices at destination points **32** that are related to process of copying, downloading, printing, or saving information packages, or, f) the detection of pressing a certain key on a keyboard device **28**, the pressing of a button, or the attempted use of other input devices (e.g., a speech recognition device, or a pen-table) at destination locations. As described above with respect to conditions c) and d), the detection of conditions e) and f) are performed by the control module **35** in conjunction with the computer's operating system, which cooperatively functions to trigger the destroyer process **46** to destruct the received electronic information package at the receiver device **32**.

In addition to specifying types of conditions for triggering the destruction of a received electronic information package at the destination computer terminal, the sender may specify one or more additional sets of conditions that must be satisfied for enabling the performance of certain operations on the received electronic information package at the destination location. As mentioned herein, types of permitted operations that may be performed include: but are not limited to, the following: a displaying operation for video data, text, picture and animation data on one or several display devices (not shown) at destination points; and, playing audio data on one or several audio playback/speaker devices **38** at destination points. The other conditions include, but are not limited to the following: g) a permission from the sender, e.g., entered as a parameter in the e-mail message, or, as a data or program attached to the message for use by the control module; and, h) the detection and identification of authorized user(s), for which access to these information packages is allowed; or, i) the detection or identification of other permissible electronic systems at destination locations that are trying to perform operations on the received electronic package content.

As depicted in FIG. **2**, the condition h) of detecting and identifying authorized user(s) to accomplish the detection of an e-mail message, the computer device **32** at the destination location and the sending device may include the monitoring of user(s) via TV cameras or video camera devices **49** that are installed at destination points. For example, video device hardware/software devices, such as video camera **49**, may be implemented to enable a sender **12** to observe users that request to read or play a content of information packages at destination points.

In a preferred embodiment, an electronic information package access operation may be enabled at the destination computer terminal **32** by implementation of a identification/authentication process **56** which executes locally as part of the controller module **35**, or remotely therefrom. The identification/authorization process **56** that enables users or

systems to access information packages may be performed in accordance with one or more of the following methods: the presentation by a user of a "pid" (personal ID) and/or passwords; and, the presentation and verification of that user's biometrics, fingerprints, and/or voice. That is, the identification/authorization process **56** implements well known techniques for verifying user's biometrics, fingerprints, and/or detected voice patterns at computer device **32**. Such techniques for verifying, identifying may include techniques such as described in commonly-owned, co-pending U.S. patent application Ser. No. 09/079,754 (YO998-033 (728-103), entitled APPARATUS AND METHODS FOR USER RECOGNITION EMPLOYING BEHAVIORAL PASSWORDS, the whole contents and disclosure of which is incorporated by reference as if fully set forth herein.

The control module **35** additionally enables systems to access information packages and/or systems that request to access information packages such as: a) systems at communication subroutines/switches that support transferring data along other communication channels to new destination points; b) automated systems that are capable to understand content of information packages to perform necessary operations that are required by these sent packages; and, c) robotic devices. Thus, the identification/authorization process **56** further includes a detection mechanism for identifying if systems that are trying to perform operations on the received electronic package content at destination points are permissible electronic systems. It is understood that the permissible electronic systems may be specified by a sender, e.g., entered as a parameter in the e-mail message, or, as a program attached to the message or information package.

According to the invention, access to electronic information packages is provided on displays **31**, or, via speakers **38** or telephone sets **39**, as shown in FIG. **1**. As shown in FIG. **3**, electronic information packages comprising visual, text, image, and/or pictorial data are displayed through window shells **59** according to known e-mail format or GUI representations, such as provided by Lotus Notes, Netscape, Microsoft Outlook, Eudora, and the like. However, it is understood that the window shell **59** will only display e-mail message content and prevent any further operations from being performed (no printing, copying, etc.). For instance, textual and pictorial data in window shells **59** may _run from beginning of the data to the end (from one end of the window shell to another).

In accordance with the invention as illustrated in FIG. **4**, an electronic information package **60** may comprise one or more of the following fields: 1) a reading time field **62** having a data structure which specifies the time in hours, minutes and seconds (HH:MM:SS) for when the message content is to be displayed or available for the recipient; 2) a Valid time interval field **64** (from <date:time> to <date:time>) which specifies the time range during which the message content may be read, i.e., if it is accessed before the specified time, the message will not be available, if expired, it will be automatically destroyed; 3) an authentication method field **66** which includes a description of the method implemented (either remotely or locally) for authenticating the recipient/user; 4) authentication data field **68** which includes data used for the verification method implemented, e.g., voice pattern, fingerprint and other biometric data; 5) the target recipient(s) field **70** which specifies one or more recipients allowed to access the message and their e-mail addresses; 6) a Sender field **72** which includes information about the person/system that sends the message; and 7) the actual body of the message **80**, i.e., electronic information content.

The system for providing remote user authentication, according to the invention, is now described in view of FIG. **5**(*a*). As shown in FIG. **5**(*a*), at step **82**, the message package is created on the sender system **12** and sent to the receiver terminal via communications channels **25**. Preferably, the entire communication between the sending and receiving end-points is encrypted. At step **84**, at the destination **32**, the receiver device processes the authentication method field **66** from the message package **60** and determines the type of the authentication method and that the authentication is to be performed remotely. After obtaining data (e.g., by obtaining a user-entered userid or password, and/or a camera image, voice-print, or a finger-print scan, etc.), the collected information is communicated back to the sender device at step **85** for processing there. Then, at step **86**, a verification of identity is be done by a query to the database **14** (FIG. **1**), visual inspection (by the active video camera system (FIG. **2**), or by using apparatus for user recognition according to techniques known in the prior art. When all the verification conditions are fulfilled, at step **88**, the sender will either grant the access to the information by sending a message, or, otherwise it may send a request to destroy the message. If authentication is successful, the message package will be _available to the recipient for the period of time specified in Reading Time field **62** (FIG. **4**), as indicated at step **89**, otherwise it will be destroyed, as indicated at step **90**.

The system for providing local user authentication, according to the invention, is now described in view of FIG. **5**(*b*). As shown in FIG. **5**(*b*), at step **92**, the message is created on the sender system **12**. Further this step **92** requires determining a list of authorized recipient(s) and the authentication method, and the retrieval of authentication data from the database **14** (FIG. **1**) at the sender terminal. Once all this information is determined and all the data required for authentication is packaged with the message in the Authentication Data field **68**, the message is then sent to the recipient terminal where it is received at step **94**. At step **94**, the authentication takes place and the results are compared with the data from the Authentication Data field **68**. A decision is made at step **95** to determine if the authentication was successful. If the authentication was successful, the message becomes available to the recipient for the period of time specified in reading time field at step **96**, otherwise it is destroyed at step **98**.

It should be understood that, local authentication is much faster then remote authentication, because, after the message is sent, it executes independent of the sender.

FIG. **6** is a workflow diagram illustrating the method executed at the receiver device for controlling e-mail access of the invention. As indicated at a first step **102**, the message package is received. Regardless of the type of the authentication specified in Authentication Method field **66**, the receiver enables the authentication method at step **104** and compares the results with the data contained in Authentication Data field **68** of the received message, as indicated at step **106**. If the authorization fails as indicated at **108**, the destroy process is executed and the message content is destroyed. Likewise, if the validation fails as indicated at **110**, the destroy process is executed. If the validation is accepted, the message content is available for display/playback. Once the message is displayed or played back, the reading time (HH:MM:SS) message field is checked and the timer mechanism invoked to enable display/playback of the message content for the specified time interval, as indicated at **118**. If the reading message time has elapsed, as indicated at **115**, the destroy process is executed and the message content destroyed. Likewise, the valid time interval is

checked at **118** to determine if the recipient has accessed the message content within the valid time period indicated by the Valid time field **64** of the message. Once the valid time interval has elapsed as indicated at step **120**, the message content is destroyed. Further, as shown in FIG. **6**, any illegal operation **121** causes the message to be destroyed and the sender to be optionally notified at step **123**. Thus, a message is available to the recipient only when successfully authenticated and only within the time period specified in Reading Time field.

While the invention has been particularly shown and described with respect to illustrative and preformed embodiments thereof, it will be understood by those skilled in the art that the foregoing and other changes in form and details may be made therein without departing from the spirit and scope of the invention which should be limited only by the scope of the appended claims.

What is claimed is:

1. A system for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said system comprising:

means for determining fulfillment of one or more certain conditions at said destination location, said means including means enabling a sender of a communicated package to visually observe a user requesting access to content at said destination location, said means including video monitoring system for generating video signals of users attempting to read or play information package content at a destination device and, a video monitoring system display device at said sending device for receiving and displaying said video signals, said condition including sender identification of an intended recipient by visual observation via said monitoring system display device; and,

control means responsive to detection of a fulfilled one or more certain conditions for enabling access to content provided in a communicated package, whereby said access includes enabling said intended recipient to perform an operation on said package content at said destination location.

2. The system as claimed in claim **1**, wherein said electronic information packages include content comprising one or more of: email messages, audio data, video data, animation data, textual data, and pictorial data.

3. The system as claimed in claim **2**, further including means for automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

4. The system as claimed in claim **3**, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals, said system further comprising means for determining elapsed time from receipt of an electronic information package, said means generating a signal for destroying the received electronic information package after a time interval has elapsed.

5. The system as claimed in claim **4**, wherein said elapsed time interval is specified by a sender at said sending device, said electronic information package further comprising a specification of one or more time-out intervals for use by said elapsed timing means.

6. The system as claimed in claim S, wherein said operations enabled to be performed on said package content at said destination device include displaying one or more of video data, text, picture and animation data via a display device at said destination location.

7. The system as claimed in claim **5**, wherein said operations enabled to be performed on said package content at said destination device include playing audio data on one or several speakers at said destination location.

8. The system as claimed in claim **3**, wherein said access includes forbidding a user to perform an operation on said package content at said destination device, said operations that are forbidden to be performed on received information packages include one or more of:

saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location.

9. The system as claimed in claim **8**, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting an attempted performance of a forbidden operation at the destination location, said destroying means automatically destroying a received electronic information package in response to said detection.

10. The system as claimed in claim **9**, wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying; downloading, printing, and saving, received electronic information packages.

11. The system as claimed in claim **9**, wherein said means for detecting an attempted performance of a forbidden operation at the destination location, includes means operable in conjunction with an operating system at said destination device, for detecting a pressing of a key on a keyboard operable for said destination device.

12. The system as claimed in claim **8**, wherein said means for determining fulfillment of one or more certain conditions at said destination device further includes means for receiving a direct command signal from a sender at a sending device, said sender command triggering destruction of said electronic information package.

13. The system as claimed in claim **8**, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, said physical hardware devices including CPU, memory or peripherals at said destination device, said destroying means automatically destroying a received electronic information package in response to said detection.

14. The system as claimed in claim **8**, wherein said means for determining fulfillment of one or more certain conditions at said destination device further comprises means for detecting a second or repeated attempted to play or display information package content, said destroying means automatically destroying a received electronic information package in response to said detection.

15. The system as claimed in claim **1**, wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying a user at said destination location for which access to these information packages is allowed.

16. The system as claimed in claim **15**, wherein said identification means for identifying a user at said destination location comprises:

means for enabling users to present a password to said system; and,

verification means for verifying a user's password prior to enabling access to said information package.

17. The system as claimed in claim 15, wherein said identification means for identifying a user at said destination location comprises means for enabling users to present a data for authentification/verification that include one or more of the following: biometrics, fingerprint, and voice data.

18. The system as claimed in claim 1, wherein said means for determining fulfillment of one or more certain conditions at said destination location includes identification means for identifying an electronic system at said destination location for which access to these information packages is allowed.

19. The system as claimed in claim 18, wherein said electronic system trying to access information packages comprises a communication process that supports transferring electronic package content via a communication channel to new destination locations.

20. The system as claimed in claim 18, wherein said electronic system trying to access information packages comprises an automated process capable of understanding information package content and performing necessary operations as required for playing said content.

21. The system as claimed in claim 18, wherein said electronic system trying to access information packages comprises a robotic device.

22. The system as claimed in claim 1, wherein said electronic information packages communicated from a sending device to a device at one or more destination locations, is communicated over a communications channel including one or more of: telephone wires, wireless channels, radio links, network data connection.

23. A method for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said method comprising:

implementing a video monitoring system for generating video signals of users attempting to read or play information package content at a destination device and, a video monitoring system display device at said sending device for receiving and displaying said video signals;

determining fulfillment of one or more conditions at said destination location, said determining including enabling a sender of a communicated package to visually observe a user requesting access to content at said destination location and identify an intended recipient by visual observation via said monitoring system display device as a condition; and,

in response to determination of a fulfilled one or more certain conditions, enabling access to content provided in a communicated package.

24. The method as claimed in claim 23, further including the step of automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

25. The method as claimed in claim 24, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals from receipt of an electronic package, said method further comprising the steps of:

determining elapsed time from receipt of an electronic information package; and,

generating a signal for initiating automatic destruction of the received electronic information package after said elapsed time interval.

26. The method as claimed in claim 25, further including the step of enabling a sender to specify said time interval.

27. The method as claimed in claim 23, wherein said step of enabling access to said content of said communicated package includes enabling a user to display one or more of video data, text, picture and animation data via a display device at said destination location, and play audio data on one or several speakers at said destination location.

28. The method as claimed in claim 27, wherein said step of enabling access to said content of said communicated package includes forbidding a user to perform an operation on said package content at said destination device, said operations forbidden to be performed on received information packages including one or more of: saving, copying and downloading the received information package content in a memory storage device and printing said package content at said at a destination location.

29. The method as claimed in claim 27, wherein said enabling step of determining fulfillment of one or more conditions at said destination device further comprises detecting an attempted performance of a forbidden operation at the destination location; and, in response to said detecting, automatically destroying a received electronic information package.

30. The method as claimed in claim 29, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of copying, downloading, printing, and saving, received electronic information packages.

31. The method as claimed in claim 29, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes: detecting a pressing of a key on a keyboard operable for said destination device.

32. The method as claimed in claim 27, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: receiving a direct command signal from a sender at a sending device for initiating destruction of said electronic information package.

33. The method as claimed in claim 27, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, said physical hardware devices including CPU, memory or peripherals at said destination device, and in response to said detecting, automatically destroying a received electronic information package.

34. The method as claimed in claim 27, wherein said step of determining fulfillment of one or more conditions at said destination device further includes: detecting a second or repeated attempted to play or display information package content, and in response to said detecting, automatically destroying a received electronic information package.

35. The method as claimed in claim 23, wherein said step of determining fulfillment of one or more certain conditions at said destination location includes the step of:

identifying a user at said destination location for which access to these information packages is allowed.

36. The method as, claimed in claim 35, wherein sad identifying stop further includes:

enabling users to present a password to said method; and,

verifying a user's password prior to enabling access to said information package.

37. The method as claimed in claim 35, wherein said identifying step further includes authenticating said user by enabling users to present biometric data on/verification that include one or more of the following: biometrics, fingerprint, and voice data, said method including comparing input biometric data with predetermined biometric data corresponding to the intended recipient.

38. The method as claimed in claim 23, wherein said step of determining fulfillment of one or more conditions at said destination location includes identifying an electronic system at said destination location for which access to these information packages is allowed.

39. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for controlling access to electronic information packages communicated from a sending device to a device at one or more destination locations, said method steps comprising:

implementing a video monitoring system for generating video signals of users attempting to read or play information package content at a destination device and, a video monitoring system display device at said sending device for receiving and displaying said video signals,

determining fulfillment of one or more conditions at said destination location, said determining including enabling a sender of a communicated package to visually observe a user requesting access to content at said destination location via said monitoring system display device and identify an intended recipient by visual observation via said monitoring system display device as a condition; and,

in response to determination of a fulfilled one or more certain conditions, enabling access to content provided in a communicated package.

40. The program storage device as claimed in claim 39, further including the step of automatically destroying a received electronic information package in response to detection of a fulfilled one or more certain conditions.

41. The program storage device as claimed in claim 40, wherein a fulfilled one or more certain condition includes detection of one or more elapsed time intervals from receipt of an electronic package, said method further comprising the steps of:

determining elapsed time from receipt of an electronic information package; and,

generating a signal for initiating automatic destruction of the received electronic information package after said elapsed time interval.

42. The program storage device as claimed in claim 41, wherein said step of determining fulfillment of one or more conditions at said destination device further comprises detecting an attempted performance of a forbidden operation at the destination location; and, in response to said detecting, automatically destroying a received electronic information package.

43. The program storage device as claimed in claim 41, wherein said step of determining fulfillment of one or more conditions at said destination device further includes:

receiving a direct command signal from a sender at a sending device for initiating destruction of said electronic information package.

44. The program storage device as claimed in claim 41, wherein said step of determining fulfillment of one or more conditions at said destination device further includes:

detecting changes in physical hardware devices that are not related to the process of displaying or playing information packages at destination locations, and in response to said detecting, automatically destroying a received electronic information package.

45. The program storage device as claimed in claim 41, wherein said step of determining fulfillment of one or more conditions at said destination device further includes:

detecting a second or repeated attempted to play or display information package content, and in response to said detecting, automatically destroying a received electronic information package.

46. The program storage device as claimed in claim 41, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes:

detecting invocation of one or several processes running in CPU or memory at said destination location that are related to one or more of: copying, downloading, printing, and saving, received electronic information packages.

47. The program storage device as claimed in claim 41, wherein said step of detecting an attempted performance of a forbidden operation at the destination location includes:

detecting a pressing of a key on a keyboard operable for said destination device.

48. The program storage device as claimed in claim 41, wherein said step of determining fulfillment of one or more certain conditions at said destination location includes the step of: identifying a user at said destination location for which access to these information packages is allowed.

49. The program storage device as claimed in claim 48, wherein said identifying step includes:

enabling users to present a password to said method; and,

verifying a user's password prior to enabling access to said information package.

50. The program storage device as claimed in claim 48, wherein said identifying step includes authenticating said user by enabling users to present biometric data on/verification that include one or more of the following: biometrics, fingerprint, and voice data, said method including comparing input biometric data with predetermined biometric data corresponding to the intended recipient.

* * * * *

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of any related appeals, interferences or judicial proceedings.